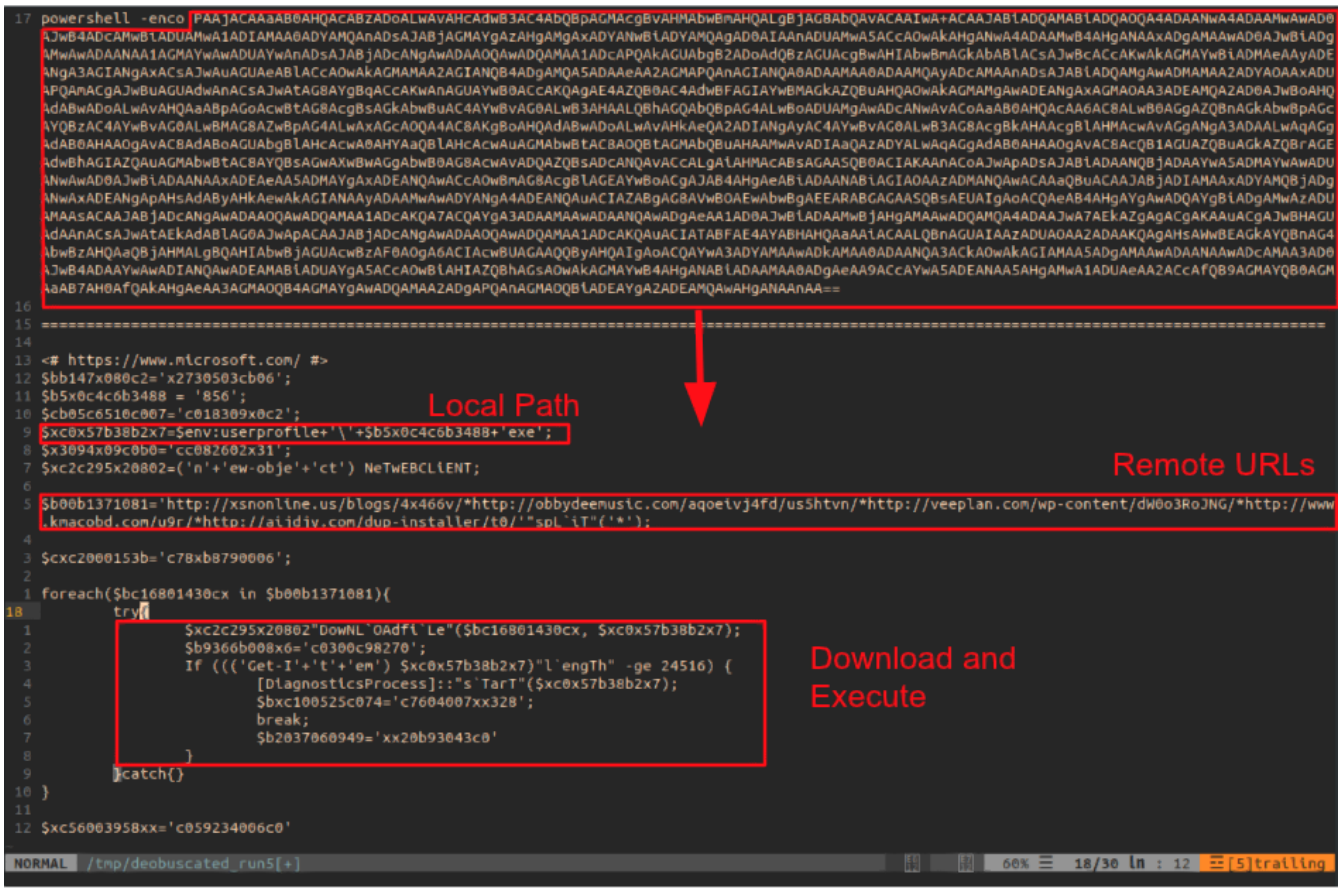
Is Emotet gang targeting companies with external SOC?

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

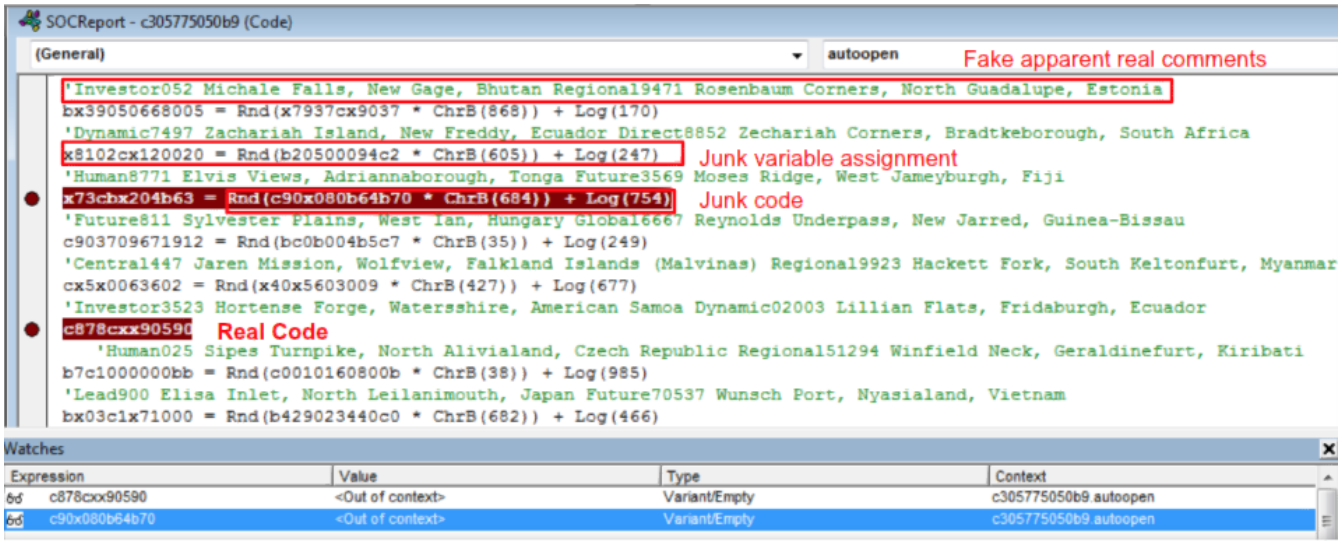
Hash	6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7
Threat	Word document Dropper (Emotet)
Brief Description	First stage of Emotet campaign targeting organization with Security Operation Centers

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.

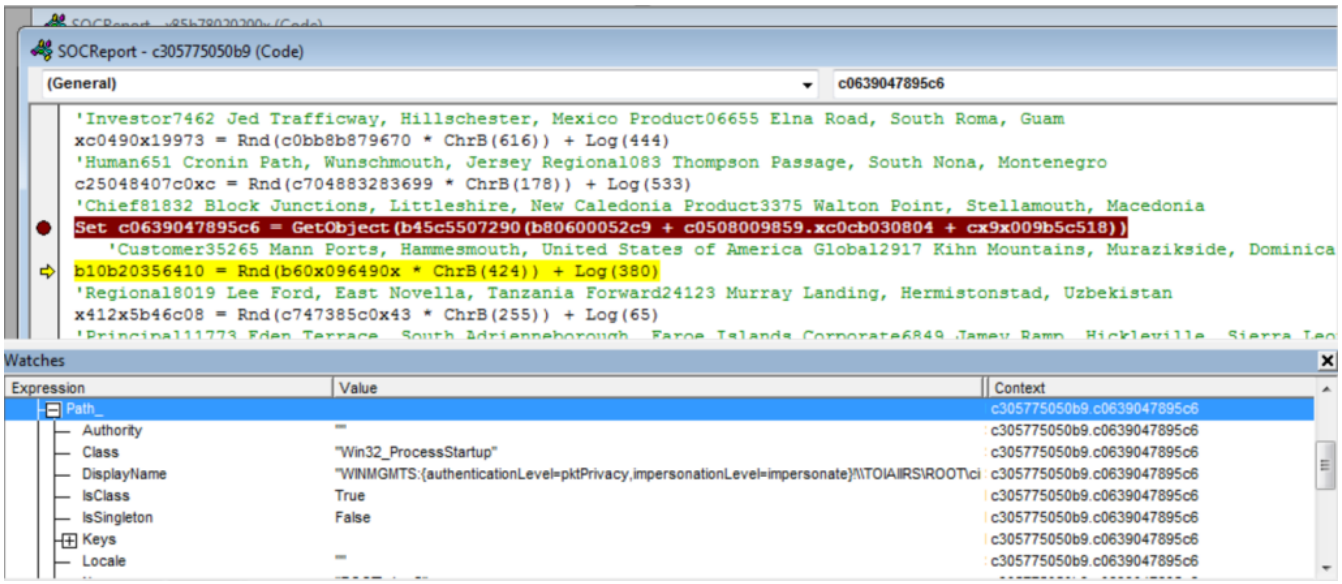
Thury-Harcourt, France. Sender IP

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.



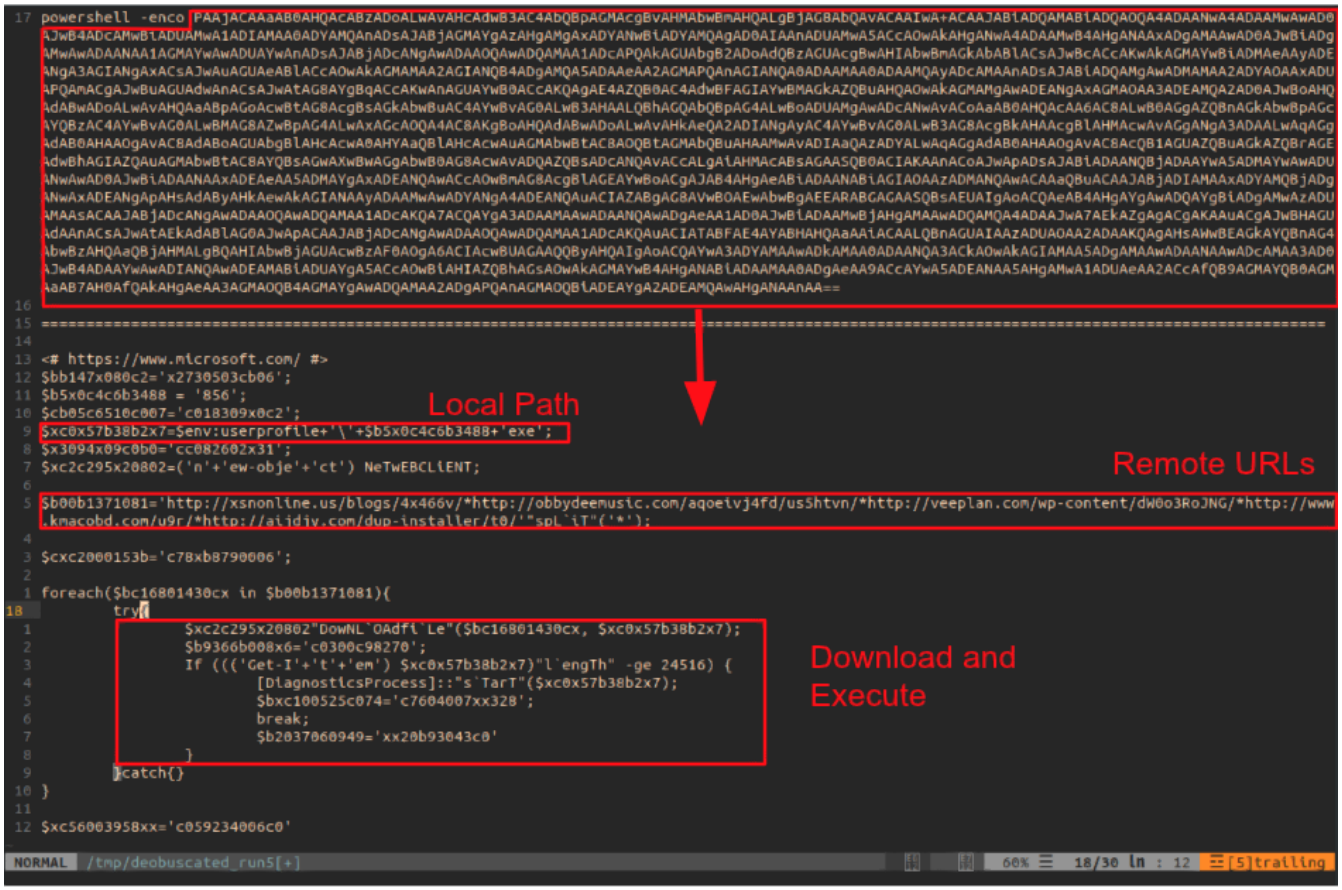
Obfuscated Macro

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.



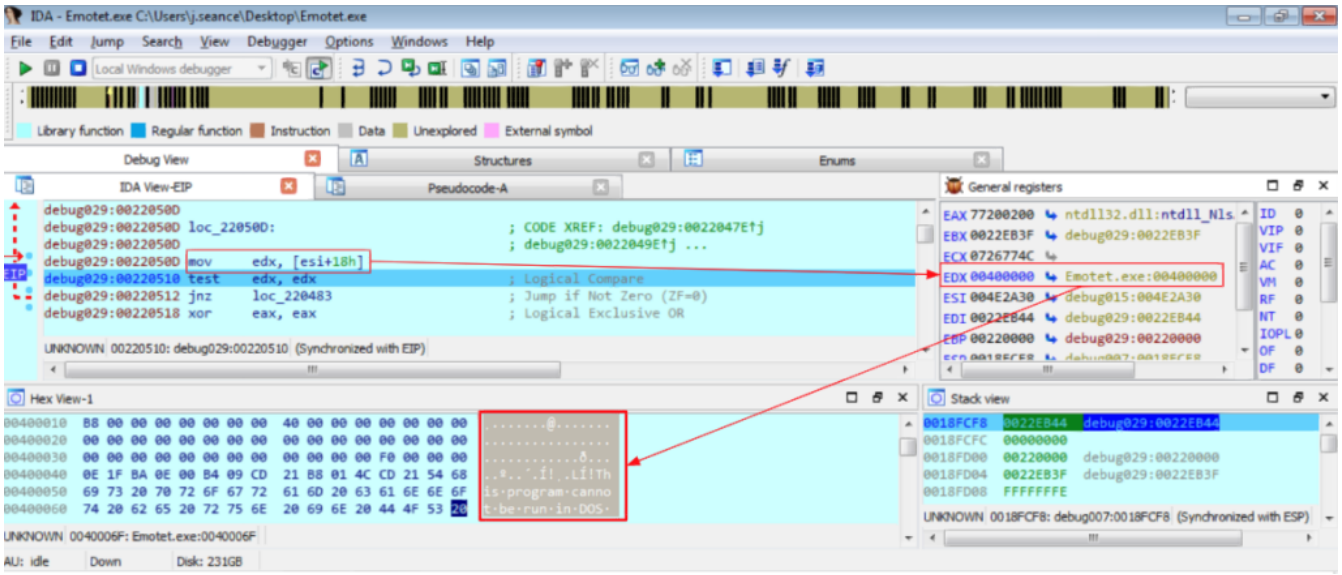
Final Deobfuscated Dropper

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)

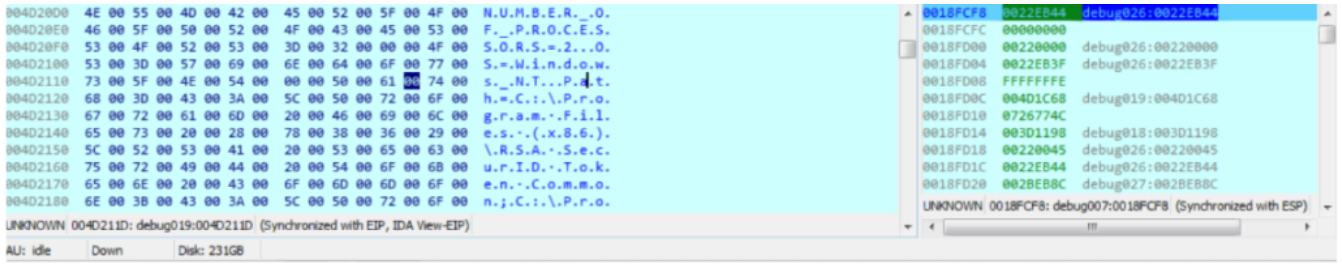
Hash	de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216
Threat	Emotet. Data Exfiltration
Brief Description	Dropped and Executed by previous stage
Ssdeep	3072:2xUIvfl2nnKJFddS2TZGjRurmOEfRtaG/70Jfm4JuLYwO9/+Tl:2lvfUnKJFddhAjYrmOEpzcflQu1+

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.



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).

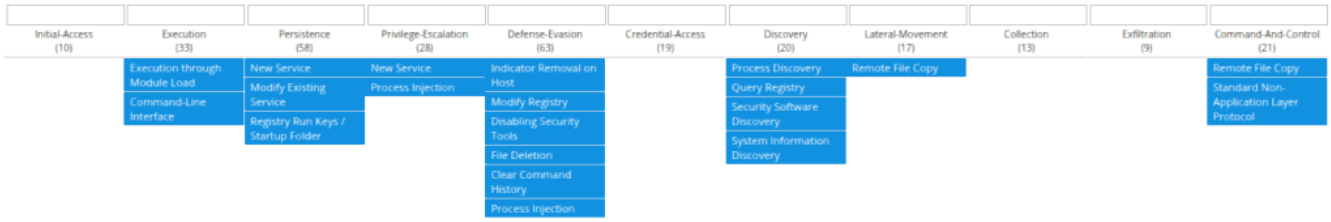


Recorded Information

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.



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+VqpDpPDXxNH3cc
 ascii
      $s4 =
"tblJgbnpgZmZCaHxmfEpoaS9Cb31DfHpZfVJobW5SYG56YGZmQmh8ZnxKaGkvQm99Q3x6WX1SaG1uUmBuemBmZkJofGZ8SmhpL0JvfUN
 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+/Eb93UVwdvrbdywicNqMdPSiMzJFXbZbSLG6cDA/O9Vy2ob3d3PeVLcie95EpT50oKkSE/8bynT1sL
 ascii
      $s6 =
"G+MfTPu8J3chkKdvVwmN7R/fNdx3H8cxWUFva2FcHweLIPfrnG/d1FcHb/FxEOQnDajHT0qu26c122W0ixunZpkE2lctqG93dy4Z7jMn
 ascii
      $s7 =
"RSVloG9h6HM56NP1tCMFZKs69gEEW+JoiOCz9U3uI3uYsb+mL2+97Wf903wpFDCKiBjjtt/TznbwXOcnHS87rh7rG4N2wHiRqPj2AReK
 ascii
      $s8 =
"iOC7W7cnZWhtQTw5nu3bSa/eHxvVFB3RfZP9CFkKs3KWazNkXJPk+HTPmTvpWFcnpLn2DUFtp2v1ELP9acqRoKOXIXMJCNtYpiEdTEP7
 ascii
      $s9 =
"6RzgkjSOWDNk6FtXIb1gBQ0oTx93sMelCVJYrG9ZEJB07FiwoYhZkKiSkNh3DQweyOCz9UXEmKjkHOXYfeRY2qT4p4UUBtCIA0+o00Fj
 ascii
      $s10 =
"StOEJiPbZbiKG6dLTcWrVy28bnd3MRHI6Se9+EtT5xnfnbI/8aimT1vHvvS1PxXYdudP5QazN3cw+OZTG6WMoPkj3ehaV6ftpUvyTw1E
 ascii
      $s11 =
"mQOhiAgYsPyI4DhFgdYtLdGQ1W9Bxmd6m3lnTJcfr4gYGLD8iOA41oOuIaXdCNnnTaphWJ1HYWqR+qqIKBiwmIjgOPiFFCgT1NbQLUTYI
 ascii
      $s12 =
"Jd812HQfx5Qv5tVrYSAcB4t1CVi1b93QVAdvpSmDyCcNpMRPSpcCbzzbZbCIG6fu/FMSVy20bHd3ShSspye94ElT56m+fUo/8bCkT1t+I
 ascii
      $s13 =
"f64odyFEoG9XrrnC4d81EHAfx9MLlPdrYegYB4s9h95Cb91oUAdvuYg3nCcNHMBPSk5z9mnbZfiNG6fklZhYVy38aXd3FwtmSie9uExT
 ascii
      $s14 =
"G5WtAP8+00dbvQhs6PgZzXSo8WjM1YD2S2wk9prpUJn8oG0I4laYrNKGZTi4kPTVMKbGcImVZllhx5Tj+amkWDhXp2+bKhvFcO9Gasz1
 ascii
      $s15 =
"3ie9qEhT593fXyw/8filT1s1hgetPxWodedPR5foK3cwiOVTG/Eyi+Yj3ZhZV6cVyoNtTw00TR93mxbYI2udnBnjHxLYp+x3IZylb1e4
 ascii
      $s16 =
"RpFqNpYQapubxqPNu6yDXrsXC6qB7CzF0GzVj0FjbT6RdW15ncWnY7/vh92xHgE5j7MjB9mZ3mVK5FiwlKhYoKj4kIq4A4DduIQLc4bc
 ascii
      $s17 =
"5Ewf7cgaGLAv7VSjeroTTJAjcpy+a7Ql2VPnU2HVntv/mUgzY6rVrB/TYQX35L9Xj+N9SPwkjLT2k+D48S0nWy/tVNKTKO5FA2W4Yy0M
 ascii
      $s18 =
"5Ewf7cgaGLAv7VSjeroTTJAjcpy+a7Ql2VPnU2HVntv/mUgzY6rVrB/TYQX35L9Xj+N9SPwkjLT2k+D48S0nWy/tVNKTKO5FA2W4Yy0M
 ascii
      $s19 =
"iBunjDe9gVct7Gx3d65SQF8nvahJU+cRqKveP/H4pE9bLL3YAz8VqHTnT7v1JHR3MIjkUxv0uwvjI92YWFenoW2yzU8NNEwfd/JCOHlr
 ascii
      $s20 =
"pKjTapsqZ36hVbhZOPU4sD5ekeEYE2WaixuncUK41ZSfp87TA/3tI91r1DvwoBcDoQywknwbTexd6FjAV+2Ac8gY7SPda9RPwKByrBsJ
 ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 800KB and
      ( pe.imphash() == "ffcd1ab4ae5e052202d6af1ea2767498" or ( 1 of ($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#Microsoft 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
}
```