McAfee Labs Threat Advisory

Emotet

December 7, 2017

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

Summary

Emotet is a Trojan Downloader spread by malicious spam campaigns using Javascript/VBScript and W97M/Downloader malware attachments. It downloads additional malware, and persists on the machine as a service. Emotet has been observed to download Ransomware, Mass Mailer worms, W32/Pinkslipbot, W32/Expiro, W32/Dridex, and Banking Trojans.

Detailed information about the threat, its propagation, characteristics and mitigation are in the following sections:

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- Restart Mechanism
- Remediation
- McAfee Foundstone Services

The minimum DAT versions required for detection are:

Detection Name	MD5 of samples	DAT Version	Date
W97M/Downloader.cdg (Spam Attachment Infection vector)	80703299ed8aeedefdb2b75ca3dd3197 4909db36f71106379832c8ca57ba5be8 4e4e9aac289f1c55e50227e2de66463b 722154a36f32ba10e98020a8ad758a7a a2a37ccac37878b490832871358c4437 067895019d23999f4ce6cda97877f771 243511a51088d57e6df08d5ef52d5499 5ad8649e4d5b1efa521d4db3509584a6 …	8604	17/07/26
Emotet-FAL	19AC1F0938EDA86935EA86B13CFCFC81 17238A77D4115A153200B352DA8667E4 A3C2BF6FFFE807C57376401F5EFCB172 …	8610	17/08/01
RDN/Ransom (Payload at time of writing)	c1182260e1ba1f930e591a98e75552d9	8471	17/03/17
Ransom-FCP (Payload at time of writing)	8fbe9a961300fb62df587ed708160655	8476	17/03/22
RDN/Ransom (Payload at time of writing)	ec8f24705dd0c58e37575a36caaa066d	8737	17/12/06

The Threat Intelligence Library contains the date that the above signatures were most recently updated. Please review the Threat Library for the most up-to-date coverage information.

Infection and Propagation Vectors

Infection and propagation are achieved through spam mail campaigns. The spam emails contain .zip files with a Javascript/VBScript inside, or an Office document with malicious macros. Customers are advised to avoid opening such files received through emails.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

McAfee Endpoint Security

Mitigation methods for assorted malware is available in the following product guide:
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

Any specific mitigation steps, if necessary, would be described later in this advisory

Endpoint Security 10.x

- Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

VirusScan Enterprise

- Refer to KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

Host Intrusion Prevention

- To blacklist applications using a Host Intrusion Prevention custom signature, see KB71329.
- To create an application blocking rules policies to prevent the binary from running, see KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, see KB71794.

McAfee Ransomware Interceptor

- To download and install McAfee Ransomware Interceptor, see McAfee Free Tools.

Characteristics and Symptoms

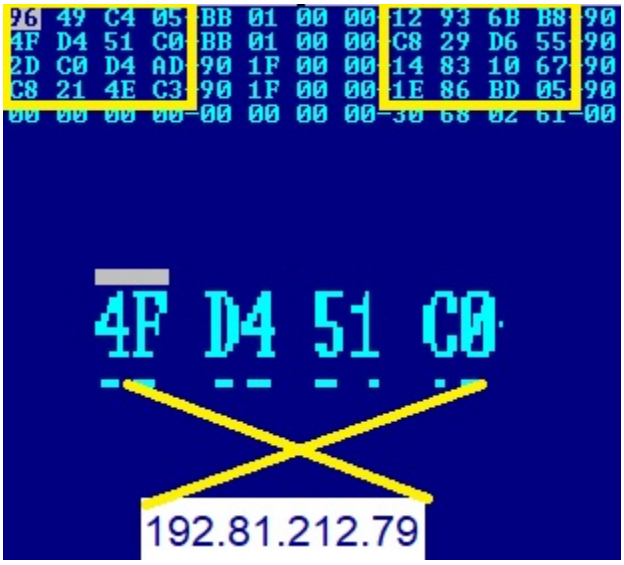
When executed on the machine, Emotet will copy itself to disk, create a service, and then attempt to reach out to its Command and Control (C&C) server for a download URL.

Location on Disk for the Dropped file:

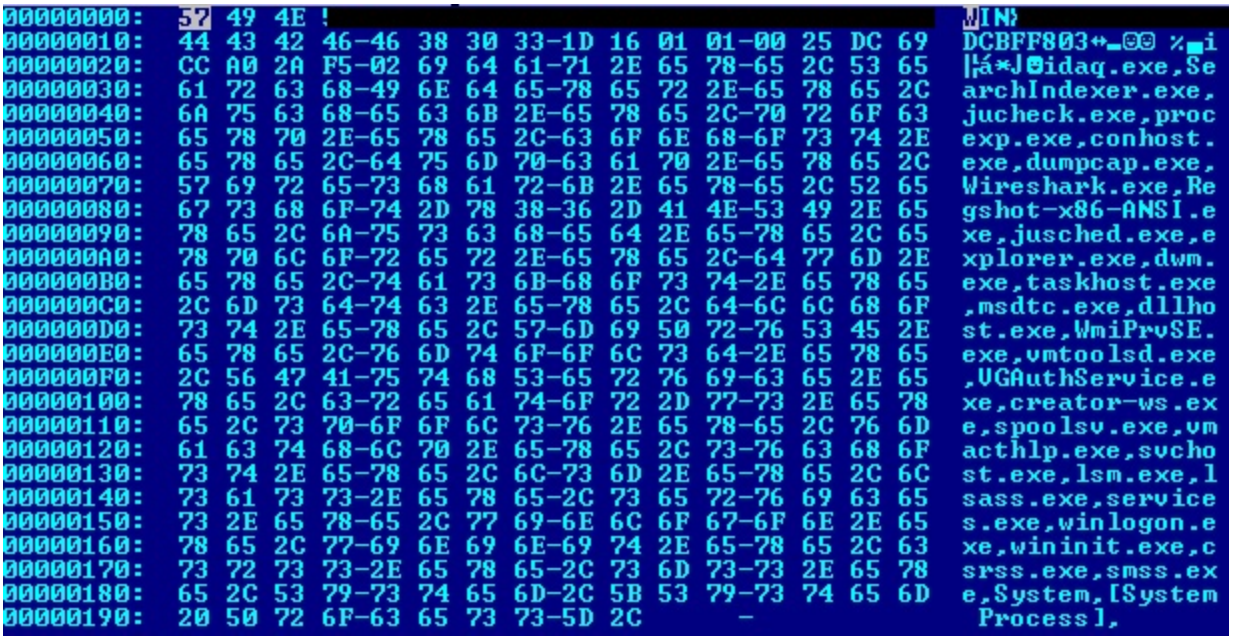
- c:\windows\system32\{Malware}.exe
- %appdata%\Microsoft\{random_folder}\{Malware}.exe
- %appdata%\services\{Malware}.exe

When the service (usually with the same name as that of the Emotet binary) is started, Emotet uses CreateTimerQueueTimer to Periodically launch new threads that connect to the C&C server. This timer lasts for 1,193 hours and starts a new thread every 100 milliseconds.

After the first successful communication with the C&C server, Emotet will check back every 15 minutes for new instructions. If it fails to contact the current C&C server, it will wait 30 seconds and attempt to connect to the next C&C server in its hardcoded list.



Emotet collects the computer name and running process information to send to the C&C server. Collected system information is encrypted and sent to the C&C server using a POST request on every communication.



C&C servers Seen in analysis:

103.16.131.20
128.31.0.39
131.188.40.189
141.138.200.249
164.132.50.32
173.212.192.45
173.212.192.45
173.230.145.224
173.243.126.142
178.254.40.5
178.62.175.211
178.79.132.214
184.107.147.18
188.166.175.18
192.81.128.131
192.81.212.79
192.81.212.79
193.23.244.244
195.191.233.221
195.78.33.200
199.21.113.151
199.21.113.151
200.33.78.195
203.150.19.63
188.241.155.6
198.154.238.174
180.131.139.203
104.236.109.186
46.101.8.170
162.243.159.58
104.236.252.178
192.81.212.79
5.196.73.150
85.214.41.200
super-sredstvo.ru (87.236.19.36)
ra-lang.ch (52.2.192.9)
nts-tech.co.kr (211.119.245.55)
septik-chistok.ru (178.210.73.230)
powerlifting64.ru (195.208.1.106)
narcoticosanonimosbolivia.org (173.254.127.241)
whiteelephanttech.com (103.195.185.222)
1000id.ru (78.108.80.117)
207.210.245.164
208.83.223.34
216.81.62.54
217.160.15.198
217.160.178.17
23.218.156.113
37.187.103.156
5.189.134.30
5.196.73.150
50.21.183.63
50.3.75.246
62.210.206.25
69.43.168.206
74.208.17.10
79.212.81.192
8.253.164.249
80.252.107.173
80.86.91.232
85.214.41.200
87.106.1.205
91.121.121.72
91.134.140.21
93.180.157.92
95.110.224.51
173.255.229.121
206.214.220.79
85.25.192.71
62.210.86.114
5.45.108.249
37.187.57.57
162.243.154.25
irishbrunettes.top (207.250.29.221)
conciergescats.top (207.250.29.221)
u1327304121722.pluton-host.ru (185.211.244.129)
cualcrisis.com (74.50.21.118)
oneacom.com (162.222.227.163)
lovesea.pl (93.157.100.77)
alexandrkogut.com (193.111.62.209)
real-clinic.ru (90.156.201.75)
seoexpert4rank.com (67.23.238.179)
inade.mx (40.78.69.25)

Emotet will contact the C&C server using an HTTP/HTTPS protocol with a POST command. The User Agents used in these requests are listed below:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
- Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; SLCC1; .NET CLR 1.1.4322)

```
POST / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: 5.196.73.150:443
Content-Length: 420
Connection: Keep-Alive
Cache-Control: no-cache

.X
n..._.jy..-."T..r.....+s?Rl`~%...1......u.#..B.x.."      E}h7..QmGPX_..}
.tA{....*...K....j.uc.DH.3...u.t....g".d.Q?.......#.n.1. .....OK.....my.+..__U.s)|Z..r?  .....3.I..@...
..;.^{B.>z_.i.#e.f?.....
....K...*.'...M...L....B..QX5@Z......x9..[G..%.-..;:..][...'.....v&....!.!t]2.../i..bk.Z9....H....g   .B......O....._
@..5L.
p.7.E.A.    ...r.&)....7...0..l....4....<E....Zm.X+./.eO.U.Y.(.\...f#.K|.........!UI....?..y.y.Ei.HTTP/1.1 404 Not Found
Server: nginx
Date: Wed, 09 Aug 2017 00:44:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 434980
Connection: keep-alive

...#cI..%..;..G.D.Ct.7.A.-.........$i....H.b..?.....B.iY..xg......3....k.       _..U..#...e
.?.......y.L.w7.._+`.y.....~-....H.Go0Q....B$.lc`..5O....4..>)~!...l'..c..wQ.fR....=..4E.ic5
nI4.~'!.=..2rCB.L?...`....ZC.....qX....o.u.C....'k......Ss.^0
......X.l..{CZ.Zra[.....!...]Q+.^....1.............92....kf....Y...N!..]:'...........]..<ec.(..............S.A.=7d..,..;..B.U...x....y.&a.<:.G..Z.Z.Ti90.O..X..."=.
1 S..[...1Sy.(.f.....u..@..%.+>7d.E..9[........O~^..J.$.s.pN0.=c_.R....q.{.4.z....I.....}\....8.A....Aac.3Y...(\D...:.L.#.mP.C.....+..(..S.B.t-V..wG|.V..`..P2.../..D.
```

The payload samples are downloaded to %Windir%\System32 using a random name. The name might be either a GUID format or a 5-digit random name.

Notes:

- %UserProfile% - C:\Documents and Settings\[UserName]
- %Temp% - C:\Documents and Settings\[UserName]\Local Settings\Temp
- %AppData% - C:\Documents and Settings\[UserName]\Application Data\Roaming
- %WinDir% - C:\Windows\
- %ProgramData% - C:\ProgramData

Restart Mechanism

Emotet Service based restart:

Emotet will delete the original launching file and copy itself to the following location:

- C:\Windows\system32\homeservice.exe

Emotet will add the below Service Key:

- HKLM\SYSTEM\ControlSet001\services\homeservice\Type: 0x00000010
- HKLM\SYSTEM\ControlSet001\services\homeservice\Start: 0x00000002
- HKLM\SYSTEM\ControlSet001\services\homeservice\ErrorControl: 0x00000000
- HKLM\SYSTEM\ControlSet001\services\homeservice\ImagePath: "C:\Windows\system32\homeservice.exe"
- HKLM\SYSTEM\ControlSet001\services\homeservice\DisplayName: "homeservice"
- HKLM\SYSTEM\ControlSet001\services\homeservice\ObjectName: "LocalSystem"
- HKLM\SYSTEM\ControlSet001\services\homeservice\Description: "Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced."

Remediation

Coverage of the Samples described in the Threat Alert are available in DAT 8610 and above.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.