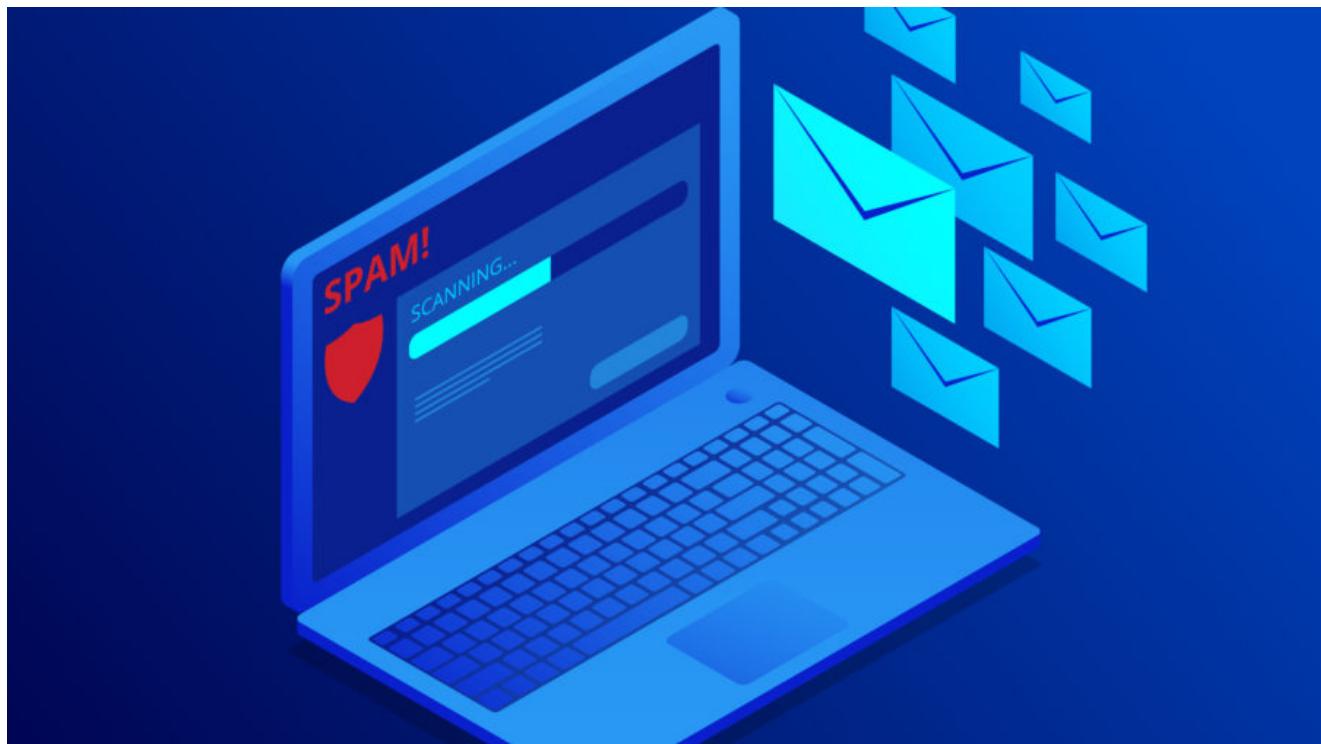


# Emotet is back: botnet springs back to life with new spam campaign

[blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/](https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/)

Threat Intelligence Team

September 16, 2019



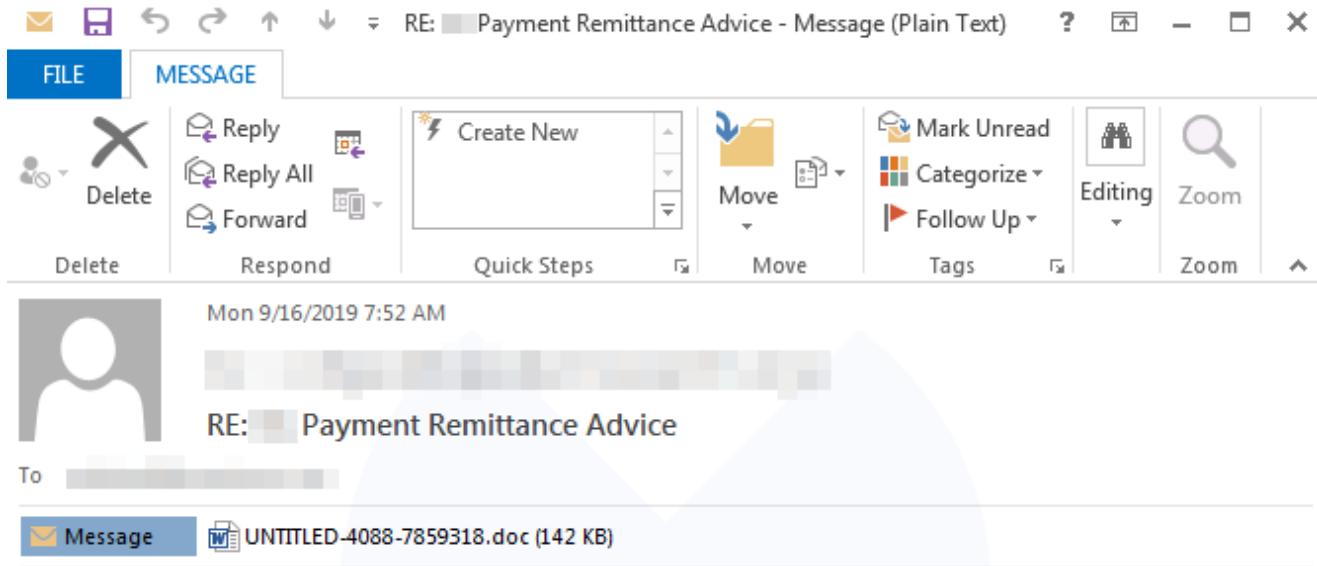
After a fairly long hiatus that lasted nearly four months, Emotet is back with an active spam distribution campaign. For a few weeks, there were signs that the botnet was setting its gears in motion again, as we observed command and control (C2) server activity. But this morning, the Trojan started pumping out spam, a clear indication it's ready to jump back into action.

The malicious emails started in the wee hours of Monday morning, with templates spotted in German, Polish, and Italian. Our Threat Intelligence team started seeing phishing emails sent in English as well with the subject line “Payment Remittance Advice.”

From	Date	Subject	Attachment(s)
[REDACTED]	2019-09-16T20:55:24.000Z	Nina [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:50:41.000Z	RE: Chiara [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:48:09.000Z	RE: [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:47:14.000Z	Tammy [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:46:44.000Z	[REDACTED], Michelle Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:42:21.000Z	Robert [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:41:26.000Z	RE: Patric [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:38:13.000Z	RE: ' [REDACTED] on Ltda. Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:36:03.000Z	Re: Beverly [REDACTED] Payment Remittance Advice	1
[REDACTED]	2019-09-16T20:33:07.000Z	RE: Chuck [REDACTED] Payment Remittance Advice	1

Figure 1: Our spam honeypot receiving Emotet emails

Note the personalization in the email subject lines. Borrowing a tactic from North Korean nation-state actors, Emotet's creators are bringing back highly sophisticated spear phishing functionality introduced in April 2019, which includes hijacking old email threads and referencing to the user by name.



Your statement is attached. Please remit payment at your earliest convenience.

If you have questions on this please contact ivc for more information.

Figure 2: The phishing email masquerading as a statement  
Victims are lured to open the attached document and enable the macro to kick-start the infection process.

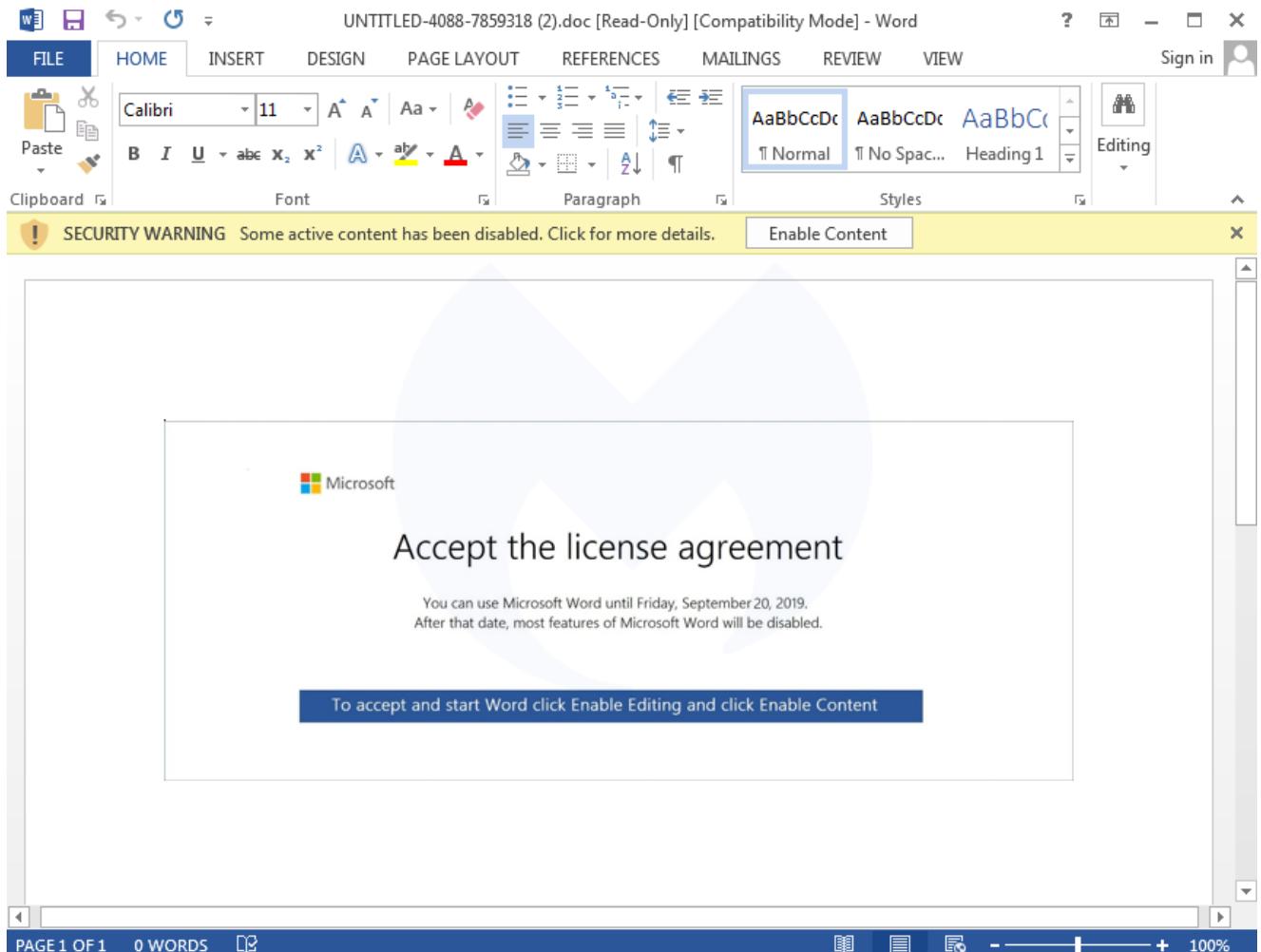


Figure 3: Word document employs social engineering to convince users into running a macro.

The screenshot shows the Microsoft Visual Basic for Applications (VBA) environment. The title bar reads "Microsoft Visual Basic for Applications - UNTITLED-4088-7859318 (2) [design]". The menu bar includes File, Edit, View, Insert, Format, Debug, Run, Tools, Add-Ins, Window, Help. The toolbar has various icons for file operations and tools. The Project Explorer on the left shows a project named "mNHWfj2" with a folder "mNHWfj2 (UNTITLED-40)" containing "Microsoft Word Objects", "Modules" (with sub-modules like Fko8Bbj, HMGckY0j, IZQ8jfTR, MHT8pjY, mzc67opG, uzdOic81, XrFtxU5q), "Class Modules", "References", and "Normal". The code editor window displays obfuscated VBA code:

```

Sub autoopen()
    On Error Resume Next
    rNZHSjPh = (oiAwLw + Rnd(947) + (4222 + Cos(8992 * Rnd(DKuk4Bf)) / 83 + I
    For Each iArs14 In DMkD685A
        For Each BVrY35a In WtzgQ71y4
            LnIAVE4 = xMfaus248 - ChrB(pvOb + Round(npy * ChrB(KYoI8IEt))) / o
        Next
        Do
            KdrHct = 512 * ChrW(M4UcTwUv) - 9232 - Sin(zpXA5n74) - hRdz53zQ -
            Loop Until fYSpVZg Eqv oWbX
        Next
        Set YEQUXnWR = mLUVi6
    Goto L1
End Sub

```

The Properties window on the left shows the "IZQ8jfTR Module" selected, with the "(Name)" field set to "IZQ8jfTR". A task manager window titled "wmiprvse.exe (1720)" is overlaid on the VBA interface, showing the following processes:

Task	Process Name	Process ID	WMI Provider Host	Path
Windows PowerShell	powershell.exe	3448	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	
768.exe	768.exe	3812	C:\Users\[REDACTED]\768.exe	
768.exe	768.exe	3360	C:\Users\[REDACTED]\768.exe	
structsgesture.exe	structsgesture.exe	2924	C:\Users\[REDACTED]\AppData\Local\structsgesture\structsgesture.exe	
structsgesture.exe	structsgesture.exe	2636	C:\Users\[REDACTED]\AppData\Local\structsgesture\structsgesture.exe	

Figure 4: Obfuscated macro code responsible for launching PowerShell

The PowerShell command triggered by the macro attempts to download Emotet from compromised sites, often running on the WordPress content management system (CMS).

There are alternate delivery techniques as well. For example, some instances of the malicious document rely on a downloader script instead.

## Document Reco...

Word has recovered the following files. Save the ones you wish to keep.

### Available Files

fb25f35c54831...  
Version created l...

Which file do I want to save?

**Close**

AGE 1 OF 1 1 WORD



# Accept the licenses

You can use Microsoft Word until Fr  
After that date, most features of Micr

Malwarebytes

Exploit automatically blocked

To ad

Affected application: 0.7055475.jse  
Protection layer: Application Behavior Protecti...  
Protection technique: Exploit payload process block...

**Close**

Figure 5: Script blocked upon macro execution

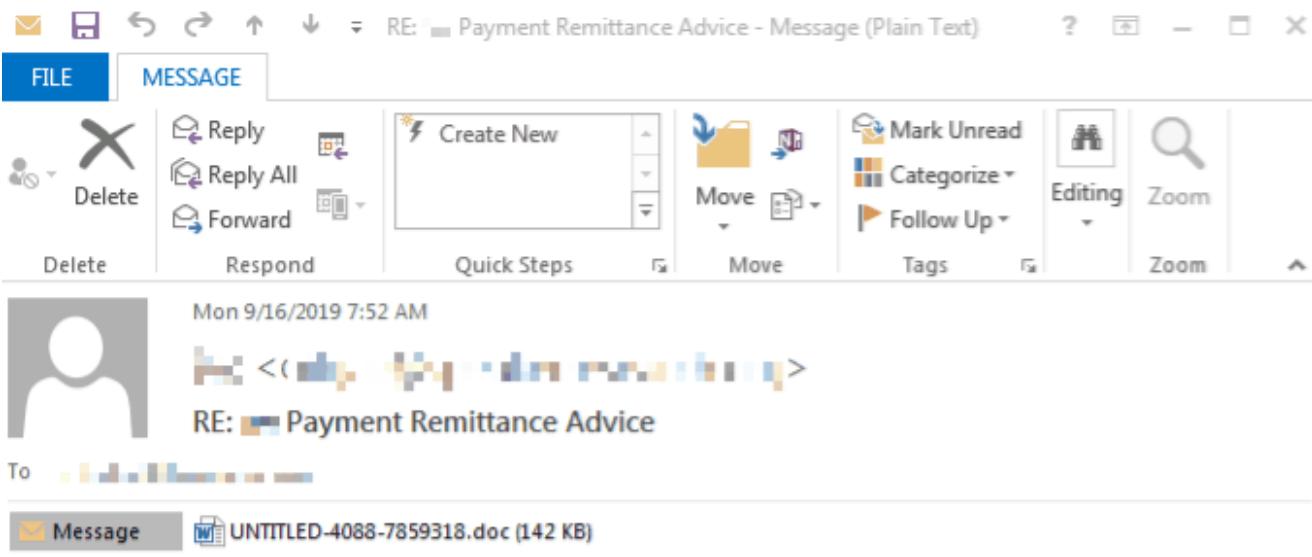
Once the download is successful and Emotet is installed on the endpoint, it begins propagating by spreading laterally to other endpoints in the network and beyond. It also steals credentials from installed applications and spams the user's contact list. Perhaps the biggest threat, though, is that Emotet serves as a delivery vector for more dangerous payloads, such as [TrickBot](#) and other [ransomware](#) families.

Emotet is most notorious for collateral damage inflicted as part of a blended attack. Dubbed the “triple threat” by many in security, Emotet partners with TrickBot and [Ryuk ransomware](#) for a knockout combo that ensures maximum penetration through the network so that valuable data may be stolen and sold for profit, while the rest is encrypted in order to extort organizations into paying the ransom to retrieve their files and systems.

Alternatively, compromised machines can lay in a dormant state until operators decide to hand off the job to other criminal groups that will demand large sums of money—up to US\$5 million—from their victims. In the past, we've seen the infamous [Ryuk ransomware deployed in this way](#).

While Emotet is typically focused on infecting organizations, individual consumers may also be at risk. [Malwarebytes business customers](#) and [Malwarebytes for Windows Premium home users](#) are already guarded against this campaign, thanks to our signature-less anti-exploit

technology. As always, we recommend users be cautious when opening emails with attachments, even if they appear to come from acquaintances.



Your statement is attached. Please remit payment at your earliest convenience.

If you have questions on this please contact ivc for more information.

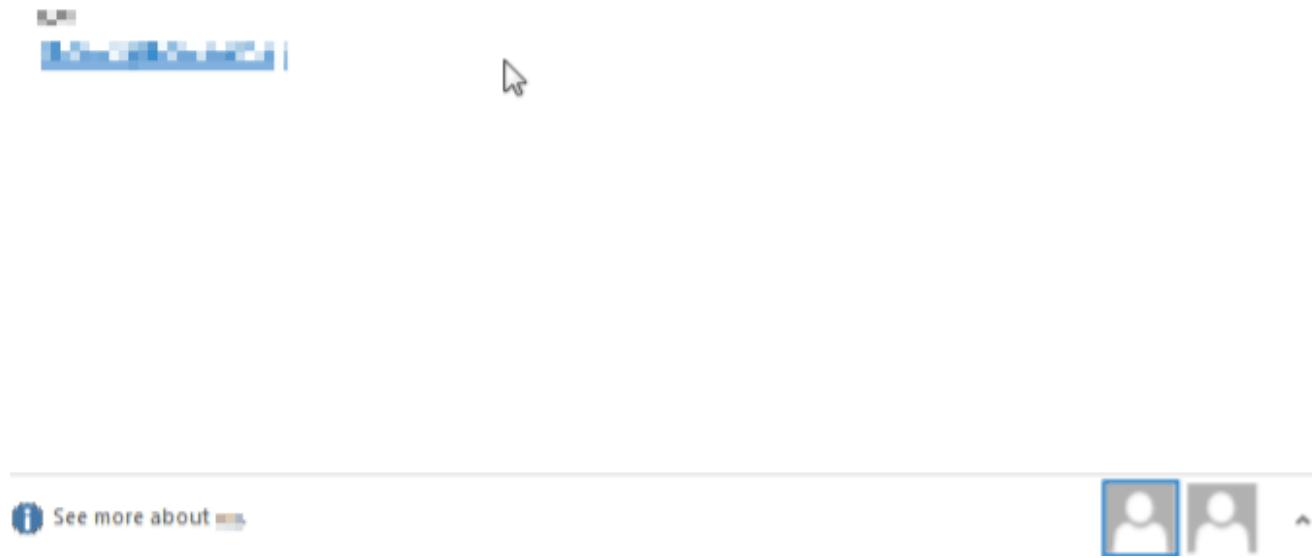


Figure 6: Malwarebytes Endpoint protection blocking the attack

## Protection and remediation

Users who are not Malwarebytes customers or who use the free scanner will want to take additional steps to protect against Emotet or clean up the infection, if they've already been hit. Businesses and organizations that may currently be battling an Emotet infection can contact Malwarebytes for immediate help. Or, for more background information on how Emotet works and a list of tips for remediation and tips, view our Emotet emergency kit.

As this campaign is not even a day old, we don't yet know the impact on organizations and other users. We will continue to update this post as we learn more throughout the day. In the meantime, warn your coworkers, friends, and family to be wary of emails disguised as invoices or any other "phishy" instances.

## Indicators of Compromise (IOCs)

---

### Email subject lines

Payment Remittance Advice

Numer Fattura 2019...

### Malicious Word documents

```
eee144531839763b15051badbbda9daae38f60c02abaa7794a046f96a68cd10b  
fb25f35c54831b3641c50c760eb94ec57481d8c8b1da98dd05ba97080d54ee6a  
bee23d63404d97d2b03fbe38e4c554a55a7734d83dbd87f2bf1baf7ed2e39e3e  
5d9775369ab5486b5f2d0faac423e213cee20daf5aaaaa9c8b4c3b4e66ea8224
```

### Hacked websites hosting the Emotet binary

```
danangluxury[.]com/wp-content/uploads/KTgQsblu/  
gcesab[.]com/wp-includes/customize/zUfJervuM/  
autorepuestosdml[.]com/wp-content/CiloXIptI/  
covergt[.]com/wordpress/geh7l30-xq85i1-558/  
zhaoyouxiu[.]com/wp-includes/vxqo-84953w-5062/  
rockstareats[.]com/wp-content/themes/NUOAajdJ/  
inwil[.]com/wp-content/oyFhKHoe  
inesmanila[.]com/cgi-bin/otxpnmxm-3okvb2-29756/  
dateandoando[.]com/wp-includes/y0mcdp2zyq_lx14j2wh2-0551284557/
```

### Emotet binaries

```
8f05aa95aa7b2146ee490c2305a2450e58ce1d1e3103e6f9019767e5568f233e  
7080e1b236a19ed46ea28754916c43a7e8b68727c33cbf81b96077374f4dc205  
61e0ac40dc2680aad77a71f1e6d845a37ab12aa8cd6b638d2dbcebe9195b0f6  
f5af8586f0289163951adaaf7eb9726b82b05daa3bb0cc2c0ba5970f6119c77a  
6076e26a123aaff20c0529ab13b2c5f11259f481e43d62659b33517060bb63c5
```

### Post-infection traffic (C2s)

```
187[.]155[.]233[.]46  
83[.]29[.]180[.]97  
181[.]36[.]42[.]205  
200[.]21[.]90[.]6
```

123[.]168[.]41[.]66  
151[.]80[.]142[.]33  
159[.]65[.]241[.]220  
109[.]104[.]79[.]48  
43[.]229[.]62[.]186  
72[.]47[.]248[.]48  
190[.]11[.]37[.]125  
46[.]29[.]183[.]211  
91[.]205[.]215[.]57  
178[.]79[.]163[.]131  
187[.]188[.]166[.]192  
181[.]188[.]149[.]134  
125[.]99[.]61[.]162  
77[.]245[.]101[.]134  
138[.]68[.]106[.]4  
187[.]242[.]204[.]142  
190[.]19[.]42[.]131  
213[.]120[.]104[.]180  
149[.]62[.]173[.]247  
181[.]48[.]174[.]242  
80[.]85[.]87[.]122  
183[.]82[.]97[.]25  
185[.]86[.]148[.]222  
90[.]69[.]208[.]50  
91[.]83[.]93[.]124  
183[.]87[.]87[.]73  
62[.]210[.]142[.]58  
186[.]83[.]133[.]253  
109[.]169[.]86[.]13  
179[.]62[.]18[.]56  
81[.]169[.]140[.]14  
187[.]144[.]227[.]2  
69[.]163[.]33[.]82  
88[.]250[.]223[.]190  
190[.]230[.]60[.]129  
37[.]59[.]1[.]74  
203[.]25[.]159[.]3  
79[.]143[.]182[.]254  
200[.]57[.]102[.]71  
217[.]199[.]175[.]216  
201[.]219[.]183[.]243  
196[.]6[.]112[.]70

200[.]58[.]171[.]51  
5[.]77[.]13[.]70  
217[.]113[.]27[.]158  
46[.]249[.]204[.]99  
159[.]203[.]204[.]126  
170[.]247[.]122[.]37  
200[.]80[.]198[.]34  
62[.]75[.]143[.]100  
89[.]188[.]124[.]145  
143[.]0[.]245[.]169  
190[.]117[.]206[.]153  
77[.]122[.]183[.]203  
46[.]21[.]105[.]59  
181[.]39[.]134[.]122  
86[.]42[.]166[.]147  
23[.]92[.]22[.]225  
  
179[.]12[.]170[.]88  
182[.]76[.]6[.]2  
201[.]250[.]11[.]236  
86[.]98[.]25[.]30  
198[.]199[.]88[.]162  
178[.]62[.]37[.]188  
92[.]51[.]129[.]249  
92[.]222[.]125[.]16  
142[.]44[.]162[.]209  
92[.]222[.]216[.]44  
138[.]201[.]140[.]110  
64[.]13[.]225[.]150  
182[.]176[.]132[.]213  
37[.]157[.]194[.]134  
206[.]189[.]98[.]125  
45[.]123[.]3[.]54  
45[.]33[.]49[.]124  
178[.]79[.]161[.]166  
104[.]131[.]11[.]150  
173[.]212[.]203[.]26  
88[.]156[.]97[.]210  
190[.]145[.]67[.]134  
144[.]139[.]247[.]220  
159[.]65[.]25[.]128  
186[.]4[.]172[.]5  
87[.]106[.]136[.]232

189[.]209[.]217[.]49  
149[.]202[.]153[.]252  
78[.]24[.]219[.]147  
125[.]99[.]106[.]226  
95[.]128[.]43[.]213  
47[.]41[.]213[.]2  
37[.]208[.]39[.]59  
185[.]94[.]252[.]13  
212[.]71[.]234[.]16  
87[.]106[.]139[.]101  
188[.]166[.]253[.]46  
175[.]100[.]138[.]82  
85[.]104[.]59[.]244  
62[.]75[.]187[.]192  
91[.]205[.]215[.]66  
136[.]243[.]177[.]26  
190[.]186[.]203[.]55  
162[.]243[.]125[.]212  
91[.]83[.]93[.]103  
217[.]160[.]182[.]191  
94[.]205[.]247[.]10  
211[.]63[.]71[.]72  
41[.]220[.]119[.]246  
104[.]236[.]246[.]93  
117[.]197[.]124[.]36  
75[.]127[.]14[.]170  
31[.]12[.]67[.]62  
169[.]239[.]182[.]217  
179[.]32[.]19[.]219  
177[.]246[.]193[.]139  
31[.]172[.]240[.]91  
152[.]169[.]236[.]172  
201[.]212[.]57[.]109  
222[.]214[.]218[.]192  
87[.]230[.]19[.]21  
46[.]105[.]131[.]87  
182[.]176[.]106[.]43