A Comprehensive Look at Emotet’s Summer 2020 Return

proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return

August 27, 2020

Blog
Threat Insight
A Comprehensive Look at Emotet’s Summer 2020 Return

August 28, 2020 Axel F. and the Proofpoint Threat Research Team

TA542, an actor that distributes Emotet malware, took an extensive break from delivering malicious emails in 2020. They were absent from the landscape for over five months, last seen on February 7 before returning on July 17, 2020. While Emotet usually takes breaks throughout the year, this was the longest known vacation for the group. Despite this break, Emotet continues to be a dangerous threat and below we've detailed their delivery methods, regional targeting, and an analysis into their use of Qbot.

Now that they are back, TA542 email campaigns are once again the most prevalent by message volume by a large margin, with only a few other actors coming close. Proofpoint has blocked hundreds of thousands of messages (sometimes coming close to one million) each day. There is no clear industry targeting among TA542 campaigns.

While there are some innovations and incremental changes, Proofpoint researchers have noted surprisingly minimal change in TA542's tactics or tooling, considering the long break. Many trends observed previously still remain relevant.

Significant new changes and innovations include:

- Distribution of Qbot affiliate "partner01" as the primary payload delivered by Emotet instead of The Trick. However, Emotet has previously delivered Qbot affiliate "hhhXX" on a few occasions such as in March 2019.
- A change in the Emotet mail sending module that can now attach benign attachments along with malicious ones.

Only small incremental changes were observed in:

- Emails: We continue to see a significant volume of thread hijacking and language localization in emails. The actor continues to use generic as well as currently newsworthy lures such as COVID-19.

- Attachments / URLs: Similar to activity observed before their break, TA542 continues to use Word attachments with macros, PDF attachments, and URLs linking to Word files.
- Country targeting: The actor continues to target a core set of countries including (listed by message volume) Germany, Austria, Switzerland, United States, United Kingdom, and Canada, while at the same time experimenting with targeting new geographies such as Indonesia, the Philippines, Sweden, and India.

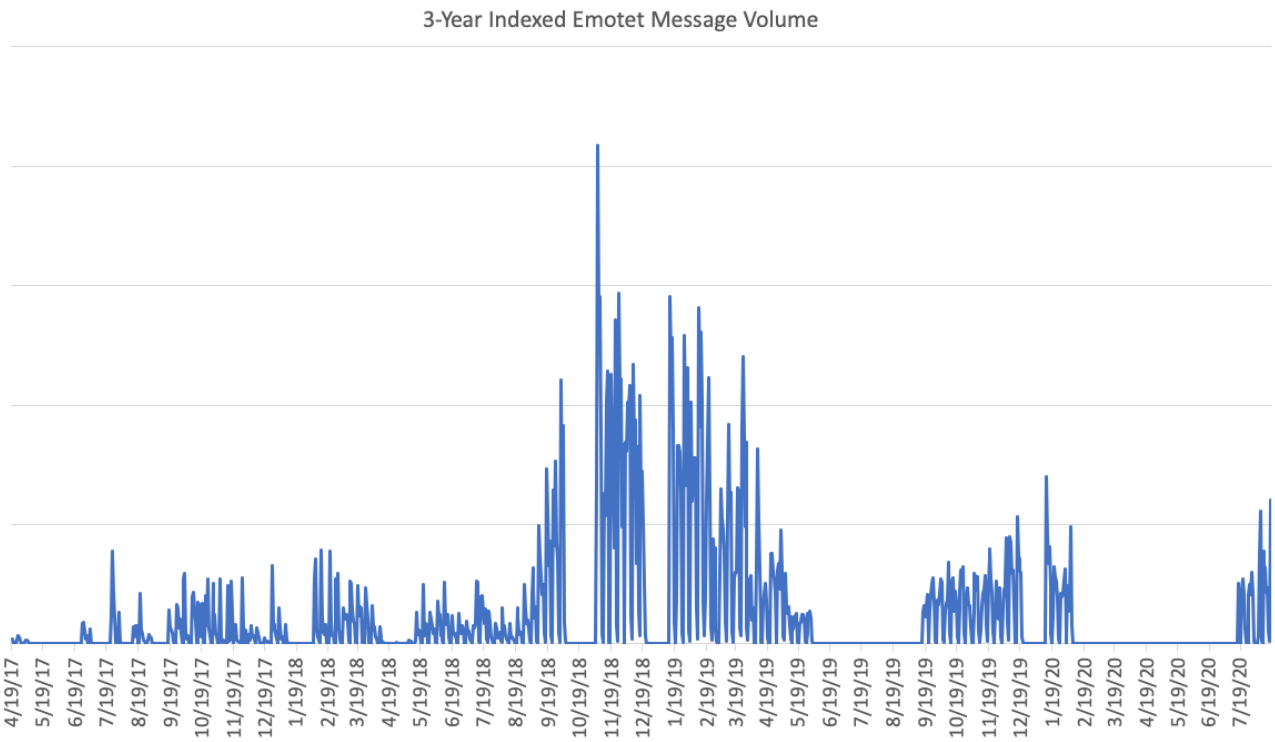

Figure 1: Indexed volume of email messages containing Emotet (from April 19, 2017 to August 18, 2020)

Precursor Campaign

Before diving into the analysis, it's important to mention that Proofpoint and other researchers were able to see warnings that Emotet was about to return. Those watching active Emotet infections took notice that new email sending modules were received. It's also possible to watch for unusual (old) Emotet email in inboxes.

On July 14, 2020 Proofpoint researchers spotted emails with old Emotet URLs, specifically those that were previously seen in the last known Emotet campaign on February 7, 2020. These emails came from many sender IPs, as if multiple emotet bots reactivated.

Delivery

Emotet malspam is very different from other malware email campaigns in that it starts early and lasts throughout the whole day, making it hard to determine the end of one campaign and beginning of the next. However, in general, campaigns start at night between **1:00am**

EST and **5:00am EST**. There are exceptions to this as some campaigns start much later in the day, for example at **3:00pm EST** on August 5, 2020.

Emotet campaigns can typically be seen Monday through Friday, and there is no significant sending on weekends. There are some exceptions to this as the actor did not send malicious email on Friday, July 24, Monday, August 3, Tuesday, August 4, or during the period of July 17, 2020 to August 18, 2020.

TA542 continues to leverage social engineering mechanisms to increase infection rates. They compose emails in the appropriate language for the targeted country. They use simple "call to action" emails.

Emails

A large percentage of Emotet emails use thread hijacking (replies to previous conversations), and the subjects begin with "Re: " or "RE: ", such as:

- Re: [subject from stolen email]
- RE: [subject from stolen email]

Another noticeable trend is using the recipient's name, job function, company name, or company domain in the subject. The Friendly-From name of the sender address often contains the company name or domain. The email body also often contains the company name, domain or recipient name in the greeting and signature.

Format	Example
[Firstname Lastname]	John Doe
[Firstname, Lastname]	John, Doe
[Companyname]	Widgetsmaker
[Companyname Recipientfunction]	Widgetsmaker Payroll
Agreement for [Companyname]	Agreement for Widgetsmaker
Files for [Companyname]	Files for John Doe
INVOICE 1067935 from [Personname]	INVOICE 1067935 from John Doe

Table 1: Example subjects that use specific information related to recipient or their company

Besides those notable trends, there is a large and varying number of subjects. Below are a few examples of other subjects, though this list is not exhaustive:

- Estimate [Digits]
- Fatura [Date]
- Financement pour
- Find attached invoice INV-Y-35852
- INVOICE [Digits]
- Nota fiscal
- Novos dados 20/07/2020
- Open Past Due Orders
- Open invoices
- Order Processing
- Our stay at the Weekend
- Outstanding Invoices
- PO 54203
- Paid Invoice & Credit Card Receipt
- Past Due Invoice
- Payroll 80606
- Question
- Quote 862639
- Quote RFQ-00012679
- Quote Request
- Renewals
- Reno Update
- Sales Invoice
- Your statement is available online
- demande

Geographical Targeting

TA542 continues the trend of consistently targeting certain regions, while also adding new countries periodically. The core regions that Emotet still targets include (listed by message volume): Germany, Austria, Switzerland, United States, United Kingdom, Japan, and Latin American countries. Other regions targeted recently but less consistently include Indonesia, the Philippines, Sweden, and India. Each country is typically targeted with appropriate language in email bodies, subjects, filenames, and branding. Known targeted countries are listed below (Table 2).

Country	Language	Note

Germany	German	Consistent targeting
Austria	German	Consistent targeting
Switzerland	German	Consistent targeting
United Kingdom	English	Consistent targeting
United States	English	Consistent targeting
Canada	English, French	Consistent targeting
United Arab Emirates	English	Consistent targeting
Japan	Japanese	Consistent targeting
Latin America	Spanish and Portuguese	Consistent targeting of countries such as Brazil, Chile, Mexico, Colombia, Ecuador
India	Hindi	Occasional
Indonesia	Indonesian	Occasional
Philippines	Filipino	Occasional
Sweden	Swedish	Occasional
Italy	Italian	Occasional
Spain	Spanish	Occasional
Norway	Norwegian	Occasional
Netherlands	Dutch	Occasional

Vietnam	Vietnamese	Occasional

Table 2: Description of the countries with observed Emotet email campaigns since July 17, 2020. Note that this list is not considered exhaustive.

Mistakes

There are often mistakes in the way that Emotet malicious emails are created, where placeholders or macros are not filled in. These may be due to bugs in the code of the Emotet mail sending capability that generates these emails. For example, we have seen attachments with names such as those listed below. Placeholders like “{rcpt.domain}” are meant to be completed in the domain.

- estimate ui00071 from {rcpt.domain-1-up}.doc
- invoice-e00889 from {rcpt.domain}.rtf.doc
- g1:regex:(invoice|profile|document|doc|doc|document|payment advice note|invoice|attn|invoice|verification letter|status update|invoice status update|invoice id|invoice for service|08_2020 invoice for service|your invoice|past due invoice|order confir.doc

There are also placeholders in the email body such as those shown below. A Spanish language email screenshot in Figure 3 illustrates this.

- {FROM.NAME}
- {MSG.MESSAGE}

Example Emails

This section highlights email lures from some of the more notable TA542 campaigns.

The figure below shows the following emails:

- Indonesian language email targeting Indonesia. The subject “faktur dari” translates to “invoice from”. (top left)
- Hindi language email targeting India and utilizing thread hijacking. The “कृपया संलग्न फॉर्म देखें।” text in the body of the email translates to “Please see the attached form.” (top right)
- Filipino language email targeting Philippines. The attachment name “impormasyon ng contact.doc” translates to “contact information.doc”. Note that this email contains both a Word attachment and a URL linking to a malicious Word file (bottom right)
- Swedish language email targeting Sweden. The subject “Dagordning för det kommande mötet på fredagen” translates to “Agenda for the upcoming meeting on Friday” (bottom left)

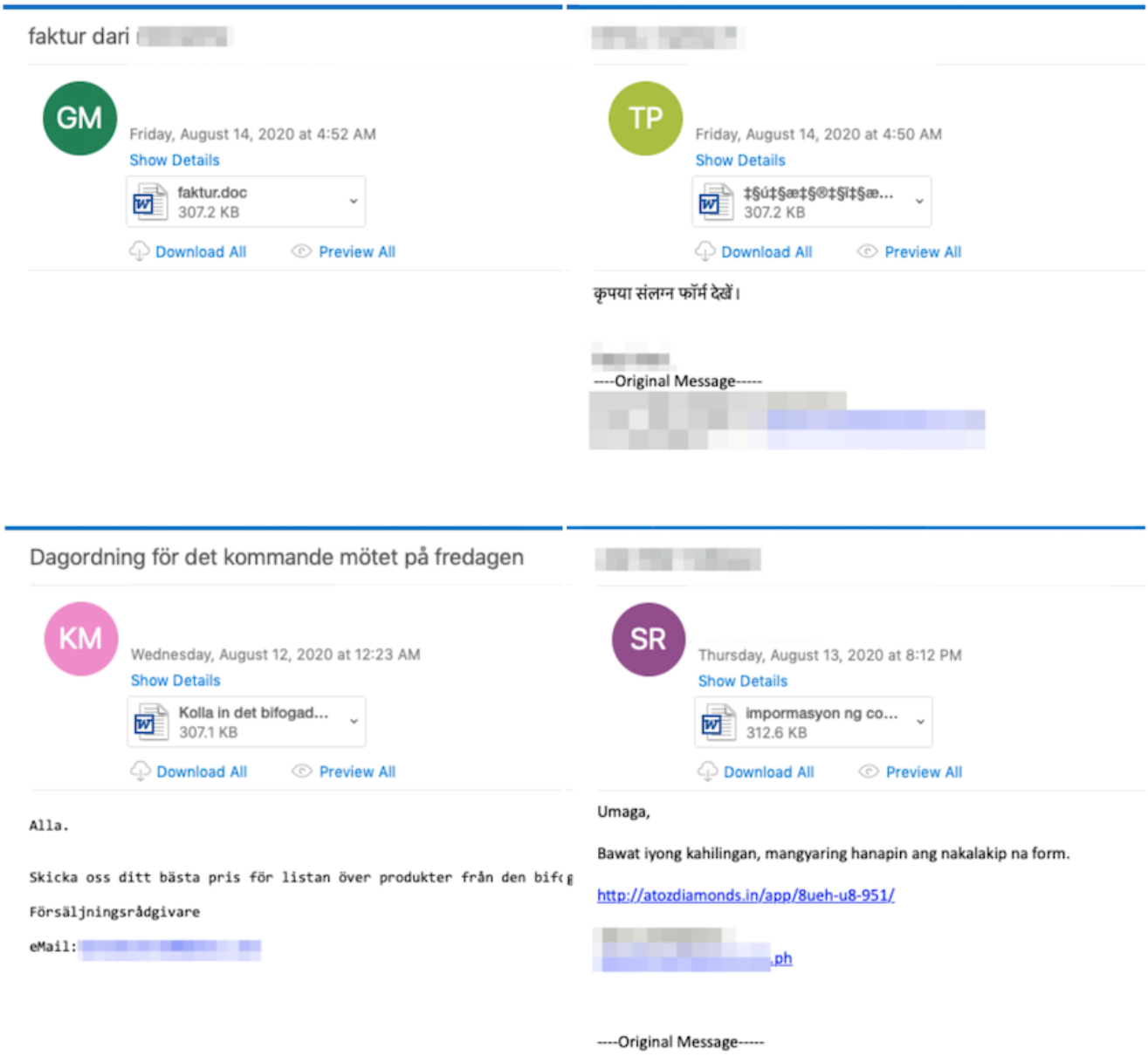

Figure 2: Clockwise, starting from top left corner, Indonesian, Hindi, Filipino, Swedish language emails.

The figure below shows the following emails:

- German language email targeting Germany. (top left)
- Spanish language email targeting Spain. Note that this email still contains the {FROM.NAME} placeholder that should have been filled in with a name before the actor sent it. (top right)
- Italian language email targeting Italy. (bottom right)
- French language email targeting Canada. (bottom left)

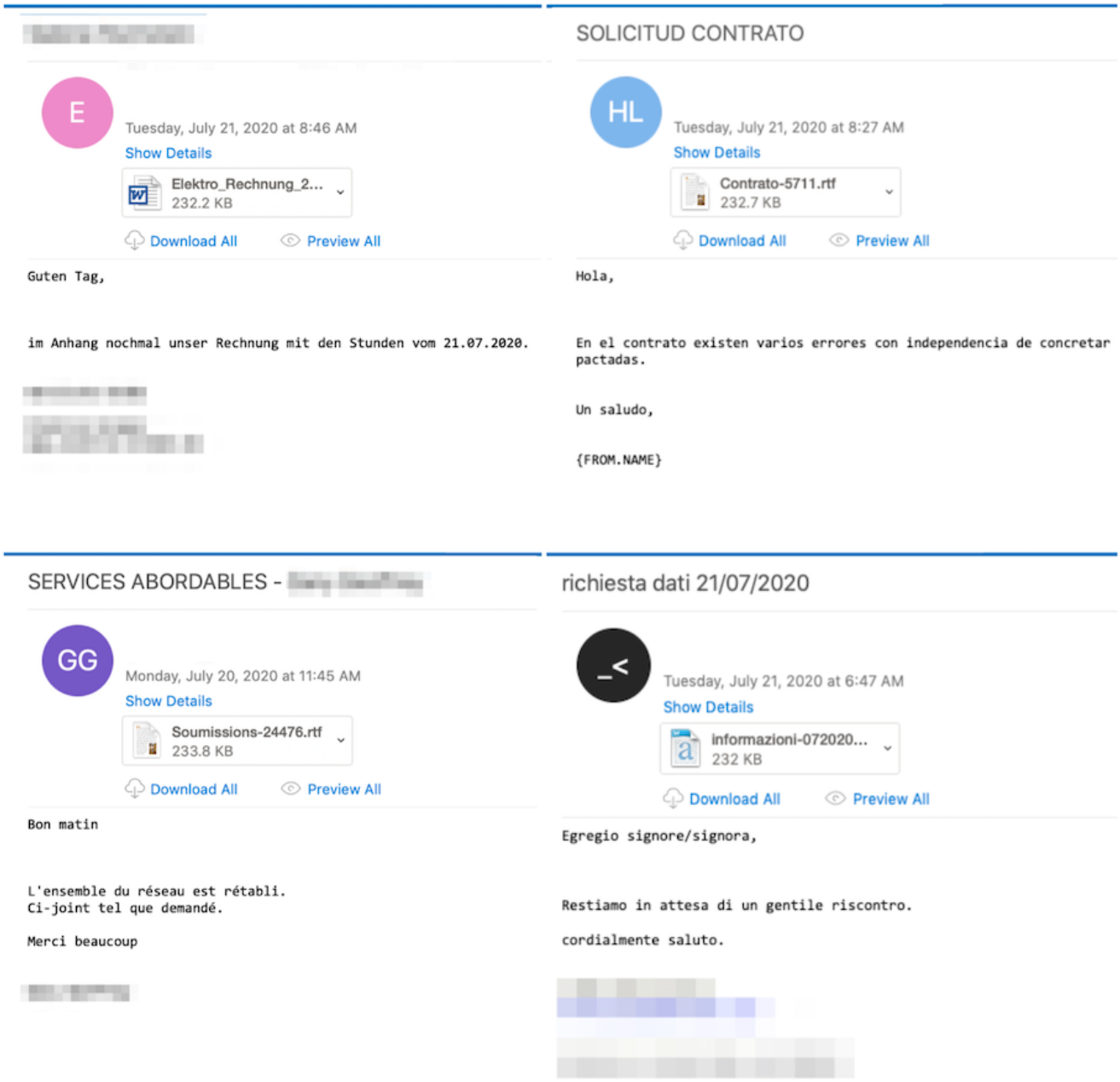

Figure 3: Clockwise, starting from top left corner, German, Spanish, Italian, French language emails.

The figure below shows the following emails:

- COVID-19 lure: On August 7, 2020 we began to see emails with attachment filenames that included “COVID-19” strings, such as “cd-8423 medical report covid-19.doc” and “covid-19 report 08 11 2020.doc”.
- Japanese Bitcoin extortion: Extortion emails in Japan are back. We saw them before Emotet took a break with an almost identical message.

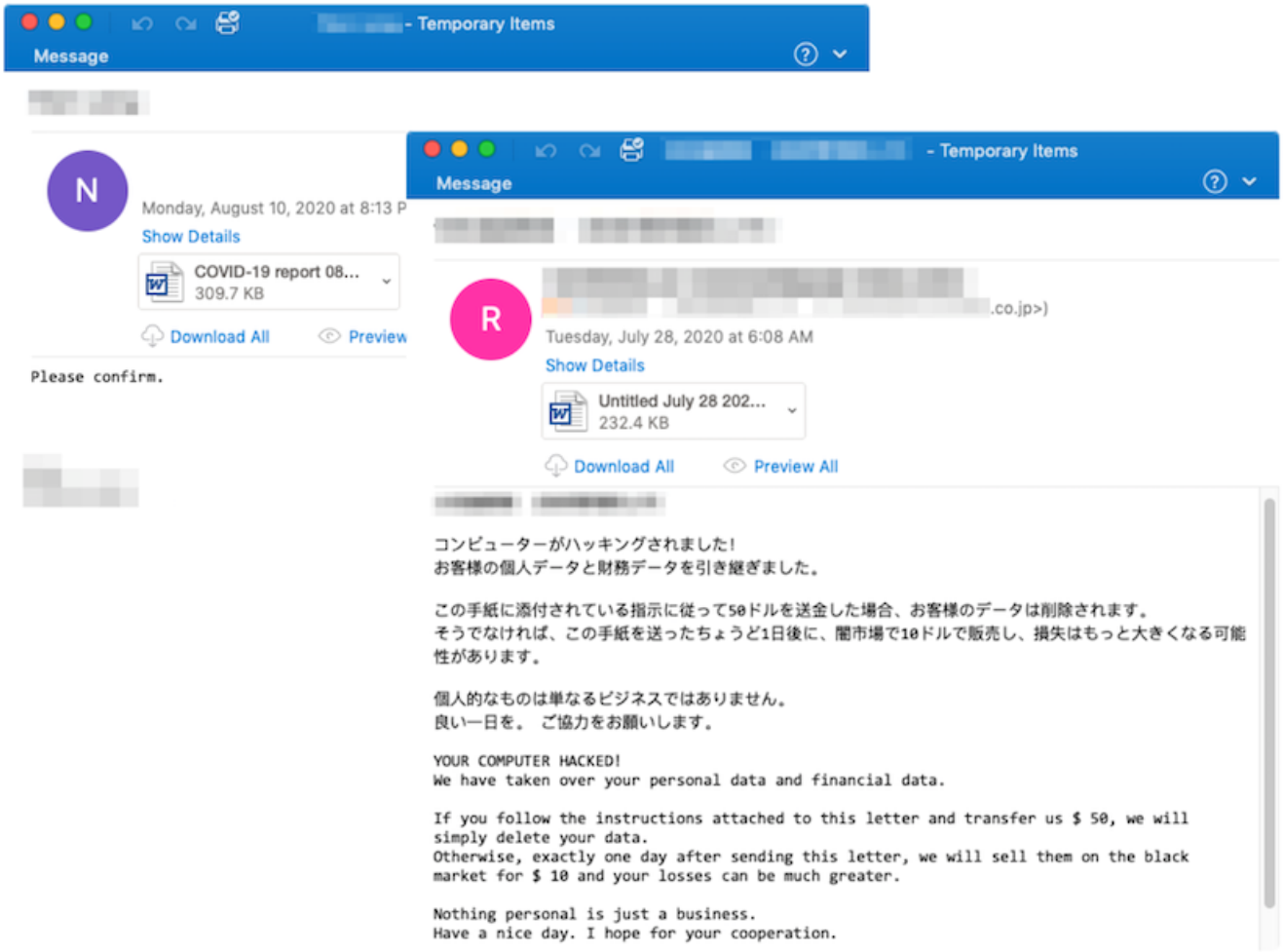

Figure 4: COVID-19 email example, Japanese Bitcoin extortion email.

We confirmed open source reports that there are examples of Emotet emails that include benign attachments along with malicious ones. These make up a minor portion of Emotet email. Examples below show benign PDF attachments along with malicious Word attachments.

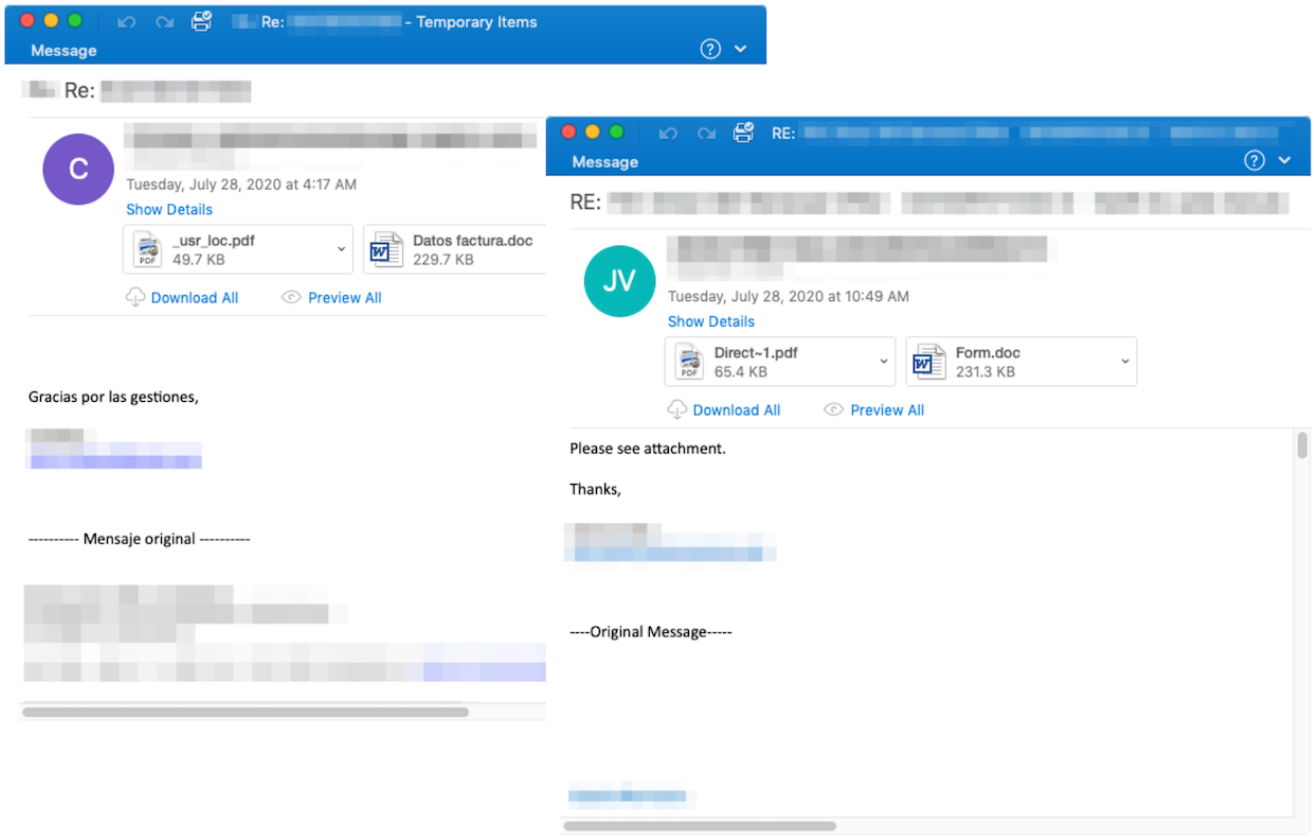

Figure 5: benign PDF attachments in the same email with malicious Word attachments.

Attachments/URLs

The malicious content included in the emails sent by this threat actor is either a URL or an attachment, and sometimes but rarely both a URL and an attachment in the same email. Word attachments are seen every day, URLs linking to Word files are also seen every day, and PDFs attachments are seen occasionally. Demonstrated for the period of July 17, 2020 to August 18, 2020:

2020-07-17: Word attachments, URLs

2020-07-20: Word attachments, PDF attachments, URLs

2020-07-21: Word attachments, PDF attachments, URLs

2020-07-22: Word attachments, URLs

2020-07-23: Word attachments, PDF attachments, URLs

2020-07-27: Word attachments, PDF attachments, URLs

2020-07-28: Word attachments, PDF attachments, URLs

2020-07-29: Word attachments, URLs

2020-07-30: Word attachments, URLs

2020-07-31: Word attachments, URLs

2020-08-05: Word attachments, URLs

2020-08-06: Word attachments, URLs

2020-08-07: Word attachments, URLs

2020-08-10: Word attachments, URLs

2020-08-11: Word attachments, URLs

2020-08-12: Word attachments, URLs

2020-08-13: Word attachments, URLs

2020-08-14: Word attachments, URLs

2020-08-17: Word attachments, URLs

2020-08-18: Word attachments, URLs

Attachments

Most often an attachment is a Word document with macros, and less commonly a PDF. Other attachment types that the actor is known to use, specifically JScript or Zips, have not been observed since Emotet returned.

The Word attachments are first-stage downloaders that attempt to download the Emotet payload using macros from one of several (typically 5) hardcoded payload URLs. A new set of five payload URLs is seen periodically, as frequently as every 1 to 2 hours. Different documents may use the same set of 5 URLs. On any given day we observe up to 100 total payload URLs.

Note: On August 18, 2020 we started observing Word files with 6 or 7 payload URLs.

The PDF attachments contain an embedded URL linking to a site hosting a similar macro Word document.

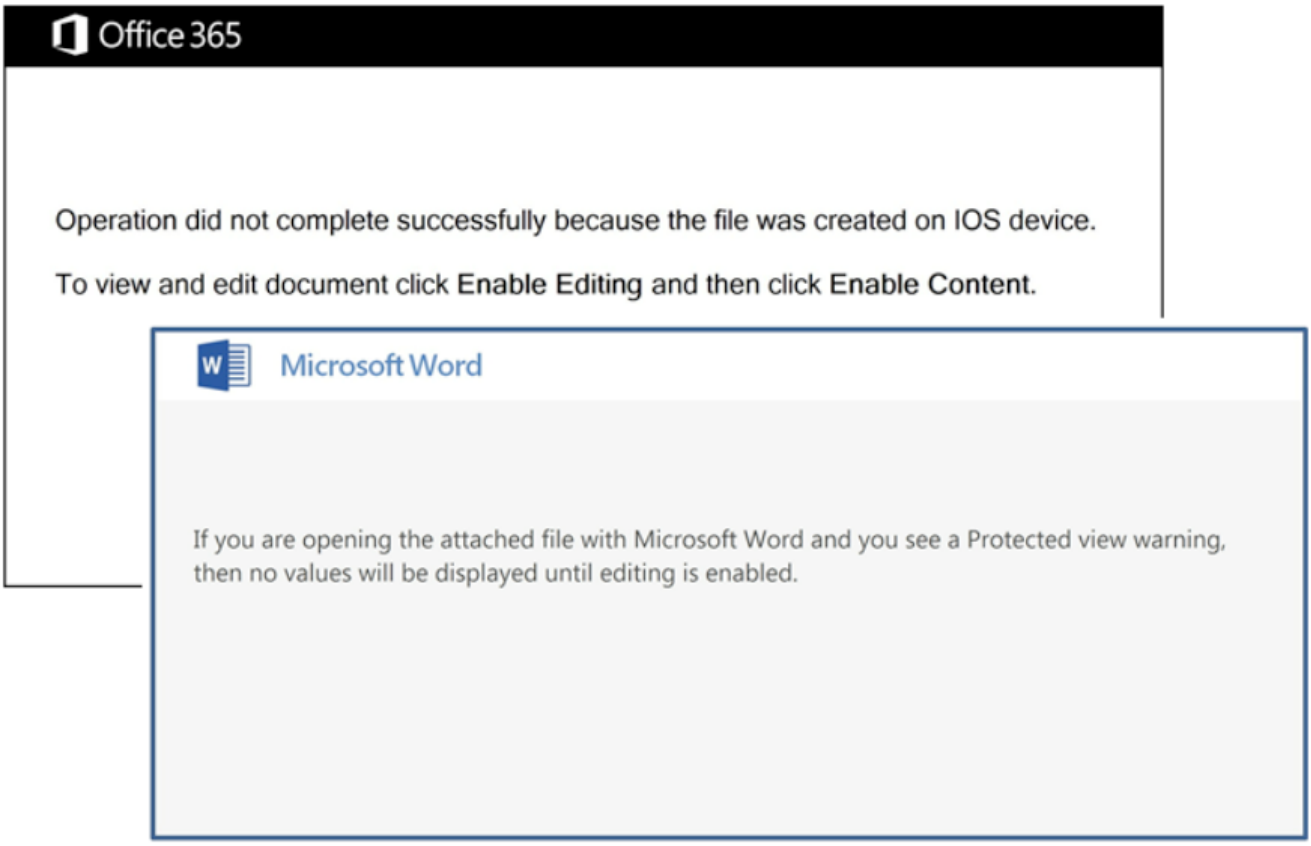

Figure 6: TA542 most commonly uses Microsoft Word documents with macros. The actor periodically updates the visual lure used in the document. This collage shows two of the observed lures.

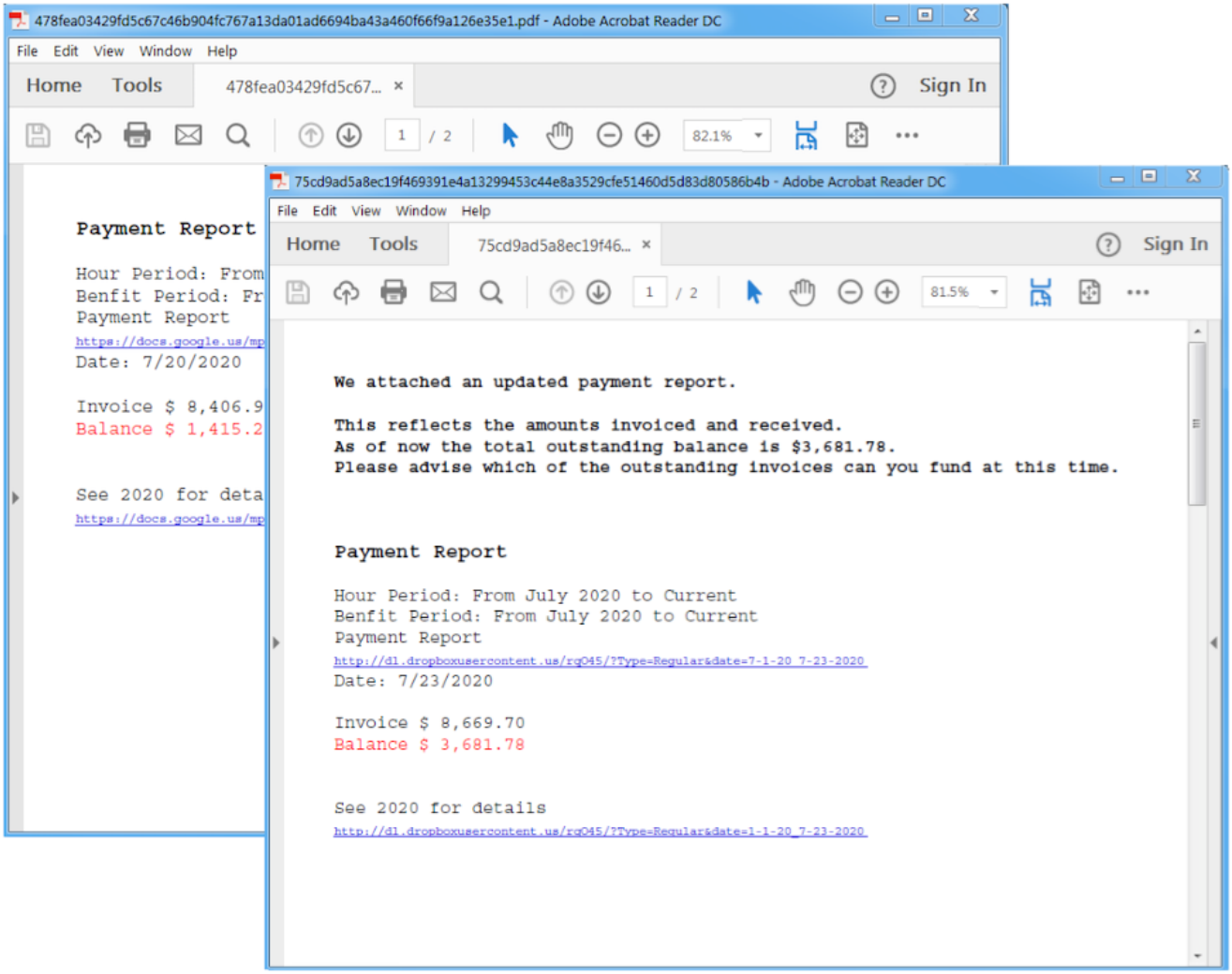

Figure 7: Examples of PDF attachments observed.

Emotet has a small library of templates for their PDF file names:

Format	Example
report.pdf	report.pdf
[2 letters]-[4 digits] report p[1 number].pdf	qx-6971 report p2.pdf
soc report [date].pdf	soc report 07 21 2020.pdf
[date]- balance & payment report.pdf	2020_07- balance & payment report.pdf

Table 3: PDF file names and format

Conversely, they have a large and varying library of file name templates that they use for the Word documents, below examples represent a small fraction of possibilities. Word attachment names are not always English–they may be in a language appropriate to the targeted geography.

Format	Example
#[5 digits].doc	#04216.doc
[5 digits] logistics rate con.doc	00089 logistics rate con.doc
[11 digits]_jul2020.doc	10068100718_jul2020.doc
[4 digits]-[5 digits]_county_report.doc	1660-63745_county_report.doc
[4 digits]-[5 digits]_city_report.doc	1850-91171_city_report.doc
[date]- balance & payment report.doc	2020_07- balance & payment report.doc
[date]- balance.doc	2020_07- balance.doc
[date]- report.doc	2020_07- report.doc
[date]- statement.doc	2020_07- statement.doc
[16 digits]_[date].doc	2873890348491143_07202020.doc
[4 digits]-[5 digits]_data sheet.doc	4087-60384_data sheet.doc
	anexo.doc
	arquivo.doc
	bank details and invoice.doc

biz_[11 digits].doc	biz_10039266887.doc
	august invoice.doc
form - [date].doc	form - aug 11, 2020.doc
zahlungsschreiben_[date]_[10 digits].doc	zahlungsschreiben_2020_08_1147364050.doc
swift_[date]_[10 digits].doc	swift_11_08_2020_6296415287.doc
sepa_[date].doc	sepa_2020_08.doc
report [7 digits].doc	report 5557308.doc
po#[6 digits] [date].doc	po#046325 110820.doc
payment summary - ref id- d[5 digits].doc	payment summary - ref id- d28114.doc
	संपर्क जानकारी.doc

Table 4: Examples of Word document file names

File names that stood out: On August 7, Proofpoint saw attachment filenames that included "COVID-19" strings, such as "**cd-8423 medical report covid-19.doc**" and "**covid-19 report 08 11 2020.doc**". These names are still in use at the time of writing.

Extension mismatches: Some emails have attachment file names with a .docm, .rtf, or .zip extension, where they should be .doc extensions. This may be accidental or a deliberate attempt to evade detection. We did not do thorough testing, but we know that Microsoft Word can open some of these attachments without errors despite the mismatch. For example, Word 2010 can open the files with .rtf extension.

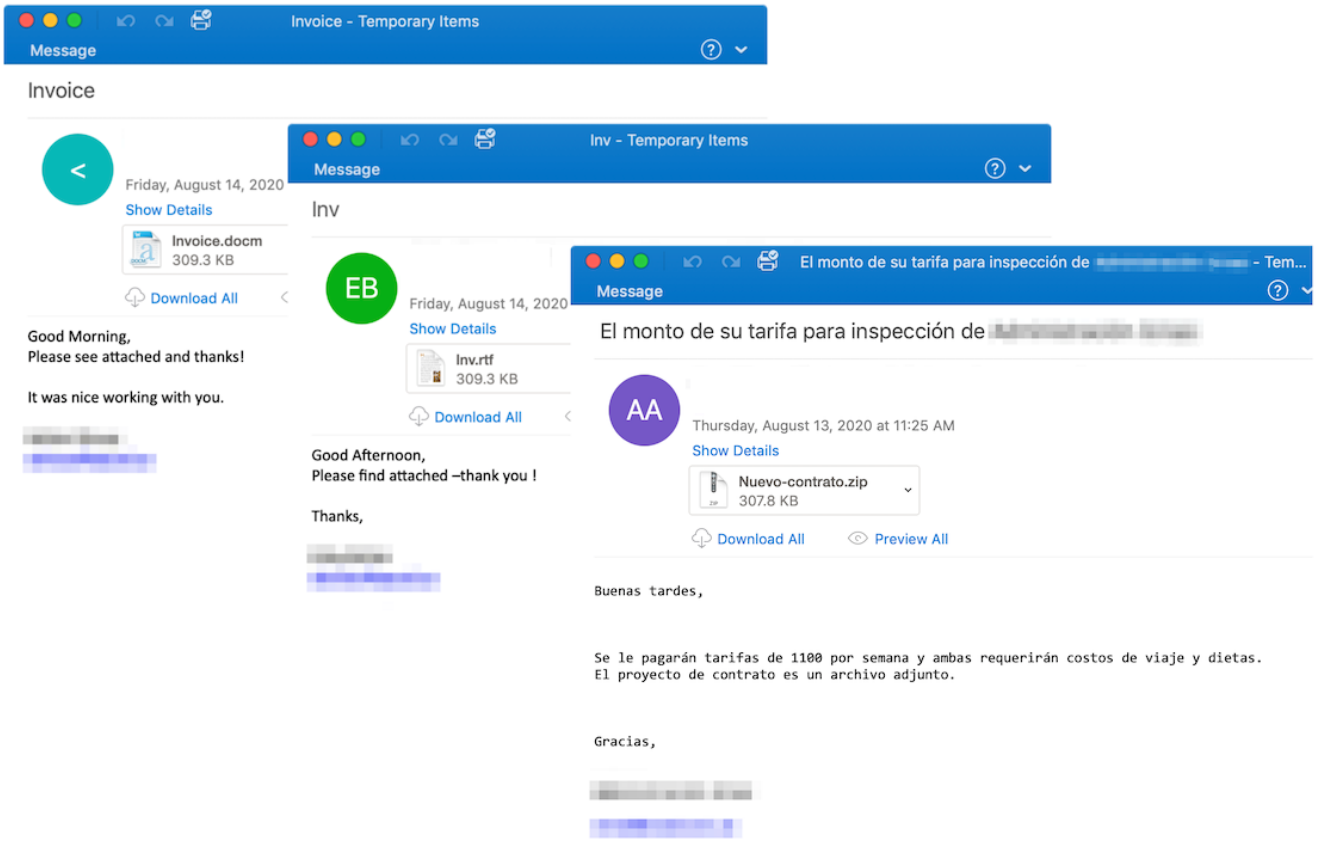

Figure 8: Example emails showing the extension mismatch

URLs

We have not observed changes in the way that this actor embeds URLs in emails. The URLs are still frequently hosted on compromised sites, including vulnerable WordPress installations. The URLs hosted on compromised WordPress CMS sites are obvious to spot as they are often hosted with “wp-content”, “wp-admin”, “wp-includes” and other similar folder structure. For other URLs it is not immediately obvious how the actor compromised the sites since there are a range of servers (i.e. Apache, nginx, IIS), databases (i.e. MySQL), languages (i.e. PHP), libraries, plugins, eCommerce frameworks, etc.

The actor typically adds a nested structure of one or more folders on the compromised site and hosts a malicious PHP script that initiates the download of the payload. Currently we only observe URLs leading to Microsoft Word documents with macros.

Malware: Emotet

We have not done extensive comparative reverse engineering and review of Emotet and its modules, but components that we analyzed had very little change. Emotet still uses the same way to store configuration and the same network command and control protocol.

We confirmed open source reports of a change in Emotet mail sending module now attaching benign attachments along with malicious attachments.

Emotet Payload: Qbot

Qbot affiliate id “partner01” is the primary payload dropped by Emotet seen almost daily. However, Emotet has previously delivered Qbot affiliate “hhhXX” on a few occasions such as in March 2019, January 2019, May 2017, and April 2017. Before Emotet disappeared from the landscape, it primarily delivered The Trick affiliate “morXX” in January and February 2020.

Example Qbot “partner01” sha256 hashes observed between July 17 and August 18:

576029dbd4166e9d6548f877bea422da5d7a07adfc5ca60c93dabbecfab3d6c7

0b2d1270ce2c5950f73ef209a08ad8e32c583e83d076509be956353bf828f03b

e999fcc1edd2cc05f82a63d4c32cc7a6fbc0fbd12de2ee82dfdd857a8a15c403

fdfa54ad4c15993944cdde7e9c37f9191c3e8eeff0e93b2c14a5973caa4dbeba

7bf42580bf8ef469a1501e53d66220542e51cc4e5af7d24e97dbc34ffe2072c2

a39c9be9acaec5e804aed2b79f937bf7e5ed6ac7220c71ca2c66decf26388cd9

a85780b23d01cb41db6f387e8351606361669bca4f669c869dee61a81333909a

b2d115a104c08eab952fc2bf342369307b89007fe24496c20378a422facb6341

cfb7d981b4782a468013b79d888ddb120b3166d4e0f2f1c4badb257ae0d233d4

02638706a6e9bdc4d62fe6d0aed441c95b19f66b4647b5e9a0aded18c17c1a64

7ca48480ca645ee2b83bf707893e84115f87ea6e327f369e40c4ab0afc8abe7a

Example Qbot configuration for the “7ca48480ca645ee2b83bf707893e84115f87ea6e327f369e40c4ab0afc8abe7a” sample:

ID: partner01

Timestamp: 1597332272

C&C: 72[.]28[.]255[.]159:995

C&C: 197[.]210[.]96[.]222:995

C&C: 71[.]192[.]44[.]92:443

C&C: 189[.]183[.]72[.]138:995

C&C: 68[.]33[.]206[.]204:443

C&C: 49[.]191[.]3[.]234:443

C&C: 71[.]56[.]53[.]127:443

C&C: 80[.]14[.]209[.]42:2222

C&C: 24[.]139[.]132[.]70:443

C&C: 76[.]187[.]12[.]181:443

C&C: 89[.]137[.]211[.]239:443

C&C: 216[.]201[.]162[.]158:443

C&C: 151[.]73[.]112[.]220:443

C&C: 92[.]59[.]35[.]196:2222

C&C: 189[.]140[.]55[.]226:443

C&C: 201[.]216[.]216[.]245:443

C&C: 50[.]244[.]112[.]10:995

C&C: 108[.]28[.]179[.]42:995

C&C: 108[.]27[.]217[.]44:443

C&C: 72[.]185[.]47[.]86:995

C&C: 199[.]116[.]241[.]147:443

C&C: 109[.]154[.]214[.]242:2222

C&C: 81[.]133[.]234[.]36:2222

C&C: 24[.]201[.]79[.]208:2078

C&C: 2[.]89[.]74[.]34:21

C&C: 50[.]244[.]112[.]106:443

C&C: 78[.]100[.]229[.]44:61201

C&C: 98[.]26[.]50[.]62:995

C&C: 174[.]104[.]21[.]157:443

C&C: 72[.]214[.]55[.]195:995

C&C: 71[.]126[.]139[.]251:443

C&C: 73[.]136[.]242[.]114:443

C&C: 86[.]99[.]75[.]165:2222

C&C: 199[.]247[.]22[.]145:443

C&C: 69[.]123[.]179[.]70:443

C&C: 41[.]97[.]231[.]7:443

C&C: 96[.]255[.]188[.]58:443

C&C: 102[.]44[.]192[.]196:995

C&C: 82[.]78[.]132[.]227:443

C&C: 75[.]135[.]184[.]133:443

C&C: 141[.]158[.]47[.]123:443

C&C: 187[.]200[.]218[.]244:443

C&C: 73[.]60[.]148[.]209:443

C&C: 185[.]246[.]9[.]69:995

C&C: 39[.]118[.]245[.]6:443

C&C: 71[.]187[.]170[.]235:443

C&C: 2[.]7[.]65[.]32:2222

C&C: 188[.]173[.]70[.]18:443

C&C: 188[.]26[.]11[.]29:2222

C&C: 2[.]89[.]74[.]34:995

C&C: 45[.]32[.]155[.]12:443

C&C: 74[.]129[.]24[.]163:443

C&C: 67[.]209[.]195[.]198:443

C&C: 67[.]246[.]16[.]250:995

C&C: 76[.]179[.]54[.]116:443

C&C: 75[.]136[.]40[.]155:443

C&C: 67[.]11[.]43[.]93:443

C&C: 94[.]49[.]67[.]180:995

C&C: 69[.]47[.]26[.]41:443

C&C: 99[.]240[.]226[.]2:443

C&C: 188[.]210[.]228[.]156:443

C&C: 173[.]26[.]189[.]151:443

C&C: 47[.]146[.]32[.]175:443

C&C: 178[.]222[.]12[.]162:995

C&C: 217[.]165[.]115[.]0:990

C&C: 68[.]116[.]193[.]239:443

C&C: 71[.]197[.]126[.]250:443

C&C: 2[.]50[.]58[.]57:443

C&C: 189[.]210[.]114[.]157:443

C&C: 207[.]255[.]18[.]67:443

C&C: 78[.]102[.]138[.]103:995

C&C: 149[.]71[.]49[.]39:443

C&C: 87[.]65[.]204[.]240:995

C&C: 96[.]232[.]163[.]27:443

C&C: 68[.]134[.]181[.]98:443

C&C: 98[.]219[.]77[.]197:443

C&C: 65[.]131[.]20[.]49:995

C&C: 66[.]30[.]92[.]147:443

C&C: 74[.]222[.]204[.]82:443

C&C: 67[.]6[.]3[.]51:443

C&C: 175[.]111[.]128[.]234:443

C&C: 200[.]124[.]231[.]21:443

C&C: 47[.]206[.]174[.]82:443

C&C: 12[.]5[.]37[.]3:995

C&C: 96[.]227[.]127[.]13:443

C&C: 134[.]0[.]196[.]46:995

C&C: 72[.]190[.]101[.]70:443

C&C: 72[.]142[.]106[.]198:465

C&C: 73[.]228[.]1[.]246:443

C&C: 2[.]51[.]240[.]61:995

C&C: 109[.]100[.]125[.]127:2222

C&C: 193[.]248[.]44[.]2:2222

C&C: 66[.]222[.]88[.]126:995

C&C: 75[.]110[.]250[.]89:995

C&C: 71[.]43[.]175[.]202:61200

C&C: 47[.]28[.]131[.]209:443

C&C: 86[.]182[.]234[.]245:2222

C&C: 186[.]82[.]157[.]66:443

C&C: 67[.]8[.]103[.]21:443

C&C: 86[.]153[.]98[.]126:2222

C&C: 73[.]137[.]184[.]213:443

C&C: 70[.]123[.]92[.]175:2222

C&C: 72[.]240[.]200[.]181:2222

C&C: 68[.]225[.]56[.]31:443

C&C: 172[.]87[.]134[.]226:443

C&C: 71[.]182[.]142[.]63:443

C&C: 72[.]142[.]106[.]198:995

C&C: 187[.]214[.]9[.]138:995

C&C: 182[.]185[.]98[.]215:995

C&C: 188[.]15[.]173[.]34:995

C&C: 68[.]190[.]152[.]98:443

C&C: 67[.]165[.]206[.]193:993

C&C: 75[.]183[.]171[.]155:995

C&C: 74[.]195[.]88[.]59:995

C&C: 96[.]41[.]93[.]96:443

C&C: 99[.]231[.]221[.]117:443

C&C: 209[.]182[.]122[.]217:443

C&C: 98[.]190[.]24[.]81:443

C&C: 209[.]137[.]209[.]163:995

C&C: 65[.]24[.]76[.]114:443

C&C: 95[.]76[.]185[.]240:443

C&C: 83[.]110[.]226[.]145:443

C&C: 74[.]75[.]237[.]11:443

C&C: 93[.]151[.]180[.]170:61202

C&C: 47[.]138[.]204[.]170:443

C&C: 98[.]173[.]34[.]212:995

C&C: 24[.]116[.]227[.]63:443

C&C: 172[.]78[.]30[.]215:443

C&C: 72[.]209[.]191[.]27:443

C&C: 76[.]170[.]77[.]99:995

C&C: 47[.]153[.]115[.]154:465

C&C: 200[.]75[.]136[.]78:443

C&C: 100[.]37[.]36[.]240:443

C&C: 77[.]27[.]173[.]8:995

C&C: 207[.]255[.]161[.]8:465

C&C: 2[.]90[.]92[.]255:443

C&C: 90[.]68[.]84[.]121:2222

C&C: 188[.]247[.]252[.]243:443

C&C: 71[.]80[.]66[.]107:443

C&C: 197[.]165[.]161[.]55:995

C&C: 73[.]227[.]232[.]166:443

C&C: 41[.]228[.]35[.]102:443

C&C: 80[.]195[.]103[.]146:2222

C&C: 65[.]48[.]219[.]244:22

C&C: 174[.]80[.]7[.]235:443

C&C: 5[.]13[.]88[.]29:995

C&C: 68[.]46[.]142[.]48:995

C&C: 24[.]28[.]183[.]107:995

C&C: 68[.]204[.]164[.]222:443

Conclusion

Since returning from an extended vacation, TA542 email campaigns are once again the most prevalent by message volume by a large margin, with only a few other actors coming close. They have introduced code changes to their malware, such as updates to the email sending

module, and picked up a new affiliate payload to distribute (Qbot). They continue to experiment with delivery to new countries. Despite these changes we also noted that many of their other methods and tooling have remained relatively unchanged from previous activity since their return. Current lures, delivery mechanisms, and widespread geographic targeting are all similar to what we have observed in the past. Whether they iterate and change their tactics or continue in the same manner, Emotet remains a highly dangerous threat.

Emerging Threats + Emerging Threats Pro Signature

2842317 - ETPRO MALWARE Win32/Emotet CnC Activity (POST) M9

Subscribe to the Proofpoint Blog