Threat Actor Profile: TA542, From Banker to Malware Distribution Service

proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service

May 15, 2019

Blog
Threat Insight
Threat Actor Profile: TA542, From Banker to Malware Distribution Service

May 15, 2019 Axel F and the Proofpoint Threat Insight Team

Update: Table 1 was updated to reflect a Poland-targeted Emotet campaign discovered on the day of publication. This is the first campaign targeting the region since 2017.

Overview

Proofpoint researchers began tracking a prolific actor (referred to as TA542) in 2014 when reports first emerged about the appearance of the group's signature payload, Emotet (aka Geodo) [1][2]. TA542 consistently uses the latest version of this malware, launching widespread email campaigns on an international scale that affect North America, Central America, South America, Europe, Asia, and Australia.

Earlier versions of Emotet had a module that was used to commit banking fraud, specifically targeting German, Austrian, and Swiss banks [7], and for years, the malware was widely classified as a banking Trojan. However, later versions of Emotet no longer loaded its own banking module, and instead loaded third party banking malware. More recently, we have observed Emotet delivering third-party payloads such as Qbot, The Trick, IcedID, and Gootkit. Additionally, Emotet loads its modules for spamming, credential stealing, email harvesting, and spreading on local networks.

TA542 typically distributes high volume email campaigns consisting of hundreds of thousands or even millions of messages targeting all industries. TA542 is currently one of the most prolific actors in the entire threat landscape. With TA542's international reach and high volume campaign strategy, we expect Emotet use to continue to grow in the upcoming quarters.

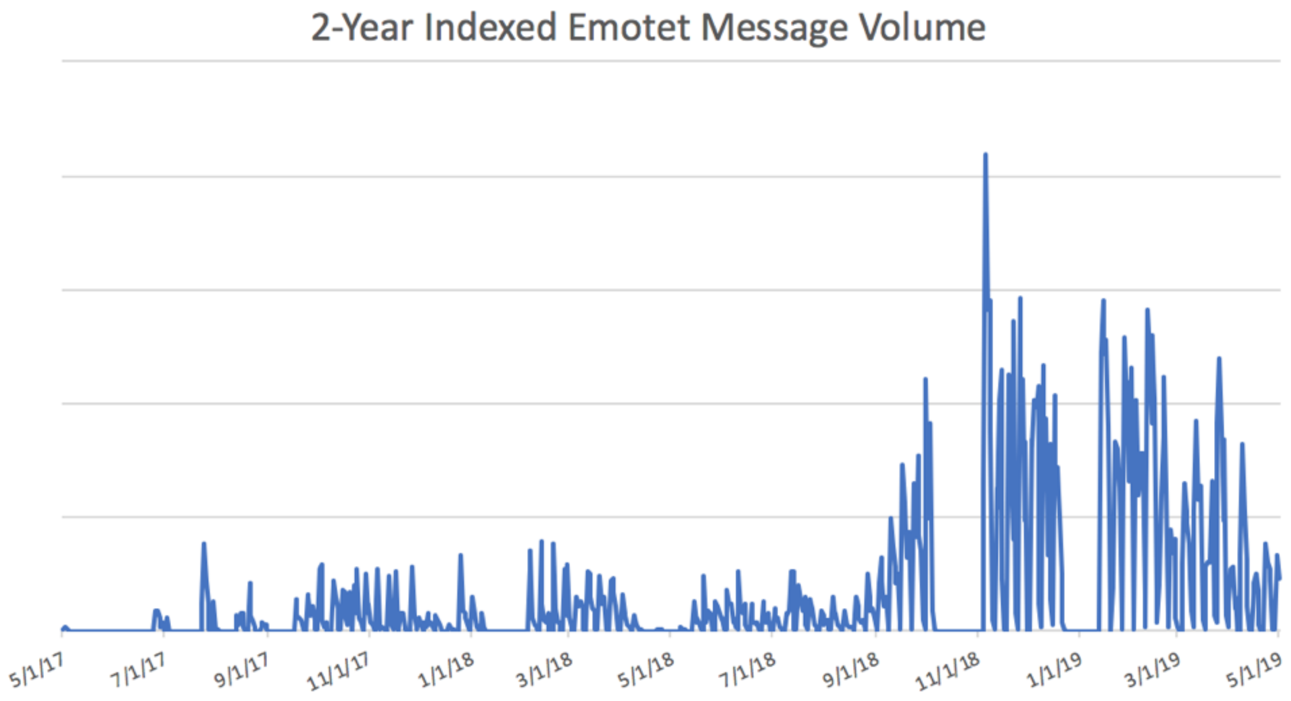


Figure 1: Indexed volume of email messages containing Emotet, TA542's signature payload (from 5/1/17-5/1/19)

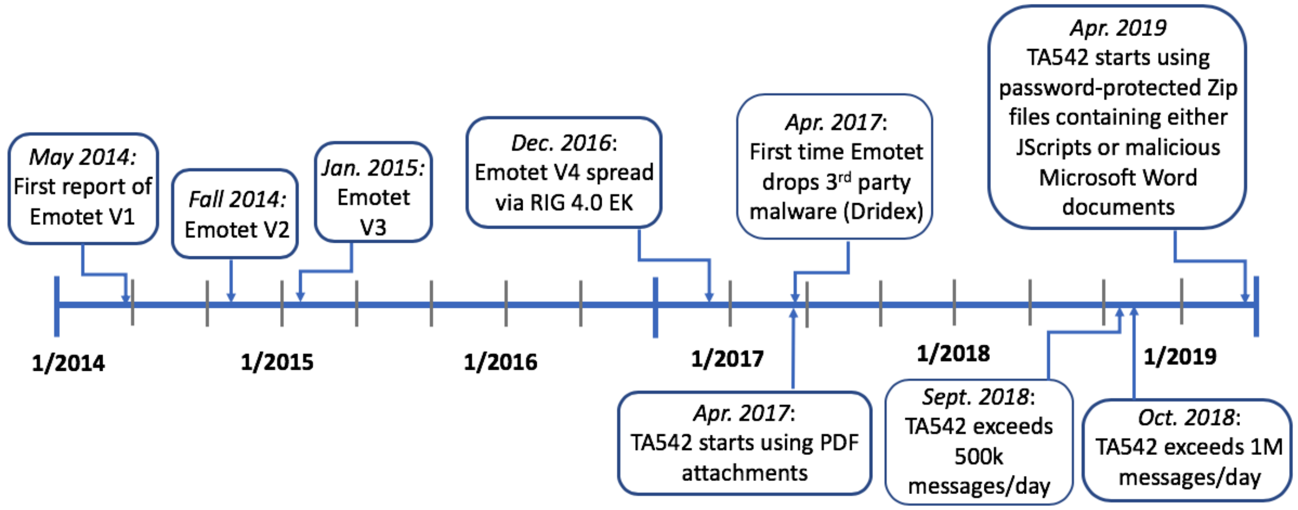
Evolution of Emotet

Version 1 of Emotet originated around May 2014 as a banking Trojan, which at first was only known to load its own banking module targeting German and Austrian banks [1][2].

Version 2 was detected in fall 2014, when it began using the Automatic Transfer System (ATS), and had a modular structure with a spamming module, banking module, DDoS module, and address book stealing module [7].

Version 3 of Emotet appeared in January of 2015, containing stealth modifications designed to prevent its detection by anti-malware defenses, and soon began targeting Swiss banks [7].

Version 4 was initially observed around December 1, 2016, spreading via the RIG 4.0 exploit kit [9]. Proofpoint researchers next observed it spreading via emails with links to zipped executables or JScript in February 2017. Starting in April 2017, TA542 began consistently distributing this version in high-volume campaigns. This version does not use its own banking module, but primarily loads other modules and third-party banking malware.



May 2014: First report of Emotet V1
Fall 2014: Emotet V2
Jan. 2015: Emotet V3
Dec. 2016: Emotet V4 spread via RIG 4.0 EK
Apr. 2017: First time Emotet drops 3rd party malware (Dridex)
Apr. 2019 TA542 starts using password-protected Zip files containing either JScripts or malicious Microsoft Word documents
1/2014
1/2015
1/2016
1/2017
1/2018
1/2019
Apr. 2017: TA542 starts using PDF attachments
Sept. 2018: TA542 exceeds 500k messages/day
Oct. 2018: TA542 exceeds 1M messages/day

Figure 2: Timeline of major milestones in TA542 activity

Emotet Modules

Since its introduction, Emotet has used a number of modules:

Main module: Downloads other modules from a command and control (C&C) server.

Spam module: This module has been present in most versions of Emotet. The spam module facilitates the continued spread of the Emotet botnet by sending out emails with links or attachments that lead to Emotet. “Distribution is performed using previously scraped mail accounts, which are sent to each spambot” from the C&C [8].

Credential stealing: This module has been present in most versions of Emotet. In version 4, it steals credentials from web browsers and mail clients, using NirSoft tools Mail PassView and WebBrowser PassView [8].

Spreader module: The network spreader module, introduced in September 2017, enumerates network resources. It attempts to connect to them “as the currently logged on user before jumping into the bruting portion of the code.” [10] The brute force attack happens by enumerating available logins and attempting passwords from a hardcoded list. For every successful login, a file is copied into the new network folder. A service is configured on the remote system to execute the file.

Email harvesting: This module was introduced in October 2018. It exfiltrates email content from the infected machines to the C&C. Specifically targeted components of email include the email subject, body, the name of the sender and the receiver, along with his or her corresponding email address. This information is only stolen for emails sent/received in the last 180 days. “If the body is longer than 16384 characters, it is truncated to this size plus the string ...” [6].

Address book stealer: This module, first seen in 2017, performs a relationship analysis between sender and recipient in the current user's Outlook data file. It extracts the name and address list from each profile's address book and then undergoes a recursive scan on each email stored in the data file. Information about each sender and recipient is extracted, which is then used to make inferences about the relationship and refine its targeting, that is then passed to the spam module. [11]

DDoS module: No longer active, a module from early versions of Emotet [7].

Banking module: No longer active, a module from early versions of Emotet [7].

Delivery

As with many threat actors monitored by Proofpoint researchers, TA542 leverages social engineering mechanisms to increase infection rates. They frequently use stolen branding and urgent subject lines in order to deceive potential victims. They also compose emails in the appropriate language for the targeted country. TA542 uses a variety of social engineering mechanisms and strategies, but the most common are described below.

Email Subjects

TA542 primarily uses generic subject lines that usually refer to transactions, payments, and invoices. Examples include: “ACH Payment Info”, “Payment Notification”, “Transaction for your invoice”, “Overdue payment”, “Paid Invoices”, “Sales Invoice”, “Status update”, “Document needed”, “New Order”, “Receipt for your invoice”.

Email Body

Often, the body of the message is simple, and consists of only a few sentences. Email bodies usually include brief verbiage about missed or upcoming payments, incoming financial statements, or invoices. However, Proofpoint researchers have observed more sophisticated examples in which TA542 included stolen company branding.

Email Thread Hijacking

Thread hijacking is a technique in which threat actors reply to existing benign email conversations with a malicious attachment or URL. Since early April 2019, TA542 began to consistently utilize this technique to distribute Emotet, sending what appear to be replies to legitimate emails [4][5]. While the technique is not novel or original, it is still effective because as victims have seen these email chains before, they may believe that they are interacting with a person they trust, making them more inclined to open attachments and links in the message body.

The appearance of thread hijacking followed reports of a new module that can steal emails from the victim's machines in October 2018 [5].

Brand Abuse

TA542 abuses the branding of dozens of high-profile companies, including them in the body of the email, Microsoft Word document attachments, PDF attachments, and in the malicious URL paths. Commonly abused brands include shipping companies (such as DHL and UPS), telecommunication companies (such as T-Mobile and O2), large financial institutions (such as TD Bank, Barclays, and RBC) and others.

Holiday Lures

TA542 also drafts holiday-themed lures to target consumers during major holidays. Proofpoint researchers have observed seasonal upticks in TA542 Emotet activity, especially around Christmas, Thanksgiving, Black Friday, and Cyber Monday, likely targeting holiday shoppers.

Geographical targeting

TA542 frequently targets certain core geographies such as Germany, United Kingdom, United States, and Latin America. TA542 also targets other countries, but less consistently. Each region is targeted with appropriate language translations in email bodies, subjects, filenames, and geographically relevant branding. Known targeted countries are listed in Table 1 below:

Country	**Language**	**Note**
Germany	German	Consistently targeted
Austria	German	Intermittently targeted: First targeted in 2015; since then intermittently targeted until April 9, 2019, when we began to observe regular targeting
Switzerland	German	Intermittently targeted: First targeted in 2015; since then intermittently targeted until April 9, 2019, when we began to observe regular targeting
United Kingdom	English	Consistently targeted
United States	English	Consistently targeted
Canada	French	Intermittently targeted

Japan	Japanese	Proofpoint observed campaigns on April 12-16, 2019
China, Hong Kong, Taiwan	Chinese	Proofpoint observed campaigns on April 12-16, 2019
Australia	English	Proofpoint observed several campaigns in April 2019
Latin America	Spanish, Portuguese	Proofpoint regularly observes countries targeted in this region, including: Mexico, Uruguay, Argentina, Colombia, Chile, Bolivia, Paraguay, Brazil, Ecuador, Costa Rica, El Salvador, Guatemala
Caribbean	Spanish	Countries such as the Dominican Republic
Poland	Polish	Last observed in 2017 *Update: Proofpoint researchers detected a campaign targeting Poland on May 15, 2019*

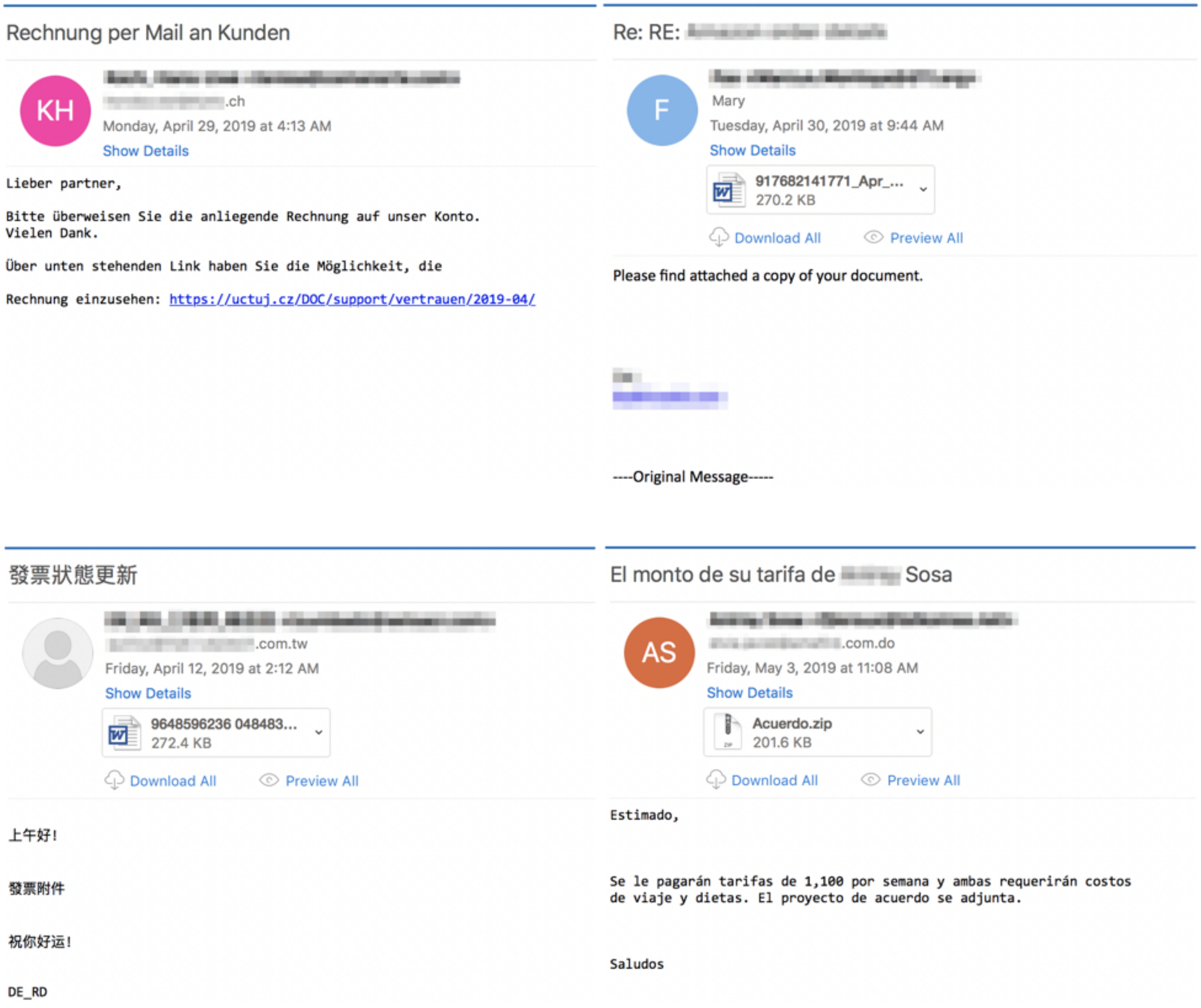
Table 1: Description of the countries with observed Emotet email campaigns. Note that this list is not considered exhaustive.

Example Emails

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

The figure below shows the following email messages:

- German language email targeting Switzerland containing a malicious URL on April 29, 2019 (top left).
- English language email targeting the United States and utilizing thread hijacking on April 30, 2019 (top right).
- Chinese language email targeting Taiwan on April 12, 2019. This email is notable because, for a few days in April, TA542 experimented with targeting this region as well as China, Hong Kong, and Australia (bottom left).
- Spanish language email targeting a company in the Dominican Republic on May 3, 2019. This particular email is notable because, while Latin American countries are frequently targeted, the neighboring Caribbean countries are rarely targeted (bottom right).



Rechnung per Mail an Kunden

KH [redacted]
[redacted].ch
Monday, April 29, 2019 at 4:13 AM
Show Details

Lieber partner,

Bitte überweisen Sie die anliegende Rechnung auf unser Konto.
Vielen Dank.

Über unten stehenden Link haben Sie die Möglichkeit, die

Rechnung einzusehen: https://uctuj.cz/DOC/support/vertrauen/2019-04/

Re: RE: [redacted]

F [redacted]
Mary
Tuesday, April 30, 2019 at 9:44 AM
Show Details
917682141771_Apr_...
270.2 KB
Download All Preview All

Please find attached a copy of your document.

[redacted]

----Original Message-----

發票狀態更新

[redacted]
[redacted].com.tw
Friday, April 12, 2019 at 2:12 AM
Show Details
9648596236 048483...
272.4 KB
Download All Preview All

上午好！

發票附件

祝你好运！

DE_RD

El monto de su tarifa de [redacted] Sosa

AS [redacted]
[redacted].com.do
Friday, May 3, 2019 at 11:08 AM
Show Details
Acuerdo.zip
201.6 KB
Download All Preview All

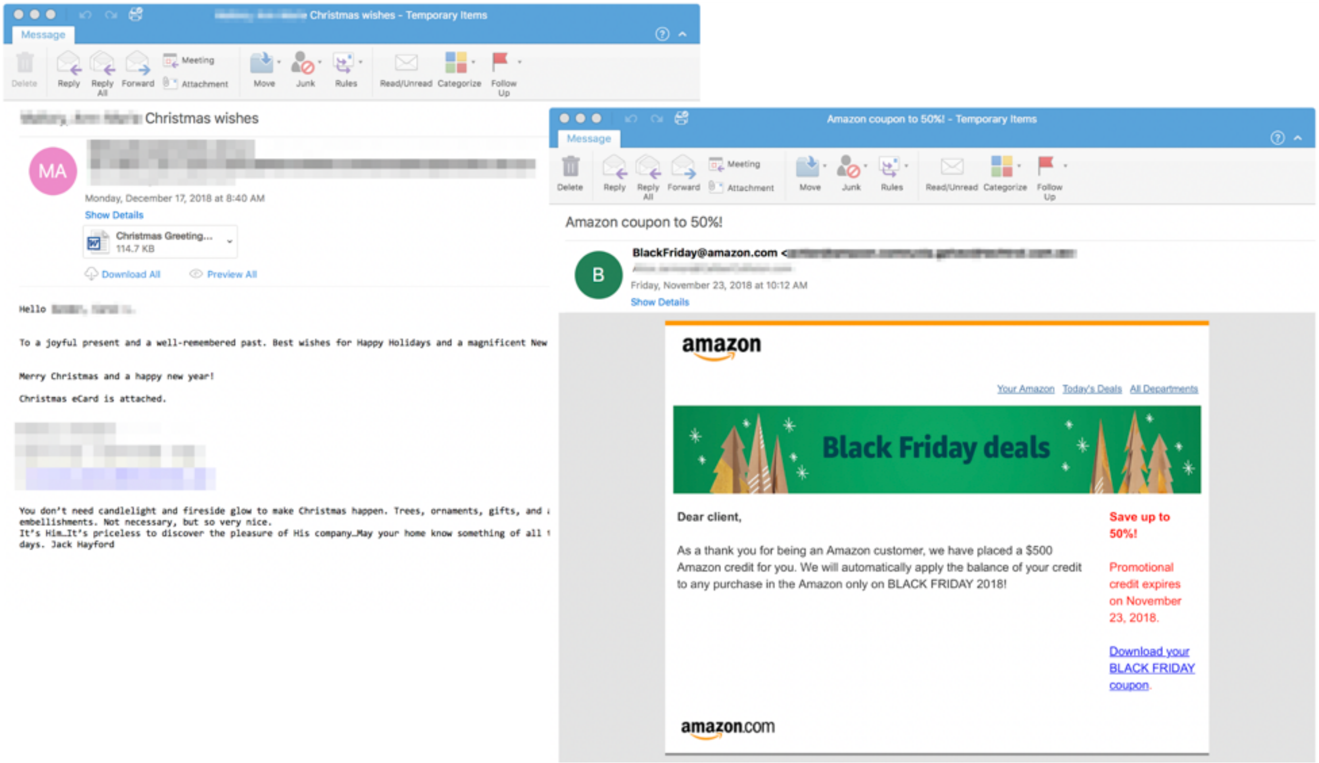
Estimado,

Se le pagarán tarifas de 1,100 por semana y ambas requerirán costos
de viaje y dietas. El proyecto de acuerdo se adjunta.

Saludos

Figure 3: Example emails showing a variety of geographic targeting by TA542, including language localization

The example emails below show the seasonal customization used in the days leading up to Christmas and Black Friday in 2018:



[redacted] Christmas wishes - Temporary Items

[redacted] Christmas wishes

MA [redacted]

Monday, December 17, 2018 at 8:40 AM

Christmas Greeting... 114.7 KB

```
Hello [redacted]

To a joyful present and a well-remembered past. Best wishes for Happy Holidays and a magnificent New

Merry Christmas and a happy new year!

Christmas eCard is attached.
```

[redacted]

```
You don't need candlelight and fireside glow to make Christmas happen. Trees, ornaments, gifts, and ‹
embellishments. Not necessary, but so very nice.
It's Him…It's priceless to discover the pleasure of His company…May your home know something of all ‹
days. Jack Hayford
```

Amazon coupon to 50%! - Temporary Items

Amazon coupon to 50%!

B BlackFriday@amazon.com <[redacted]

[redacted]

Friday, November 23, 2018 at 10:12 AM

amazon

Your Amazon Today's Deals All Departments

Black Friday deals

Dear client,

As a thank you for being an Amazon customer, we have placed a $500 Amazon credit for you. We will automatically apply the balance of your credit to any purchase in the Amazon only on BLACK FRIDAY 2018!

Save up to 50%!

Promotional credit expires on November 23, 2018.

Download your BLACK FRIDAY coupon.

amazon.com

Figure 4: Example emails showing holiday email lures

Attachments / URLs

The malicious content included in the emails sent by this threat actor is generally either a URL or an attachment, although Proofpoint researchers have observed some instances in which both were included at the same time. The actor maintains a diverse arsenal of attachments and URLs in order to vary their attacks. TA542 frequently uses some formats, such as attached Microsoft Word documents with macros and URLs linking to similar documents. The actor uses other formats such as PDFs and JScript intermittently. Finally, formats such as password-protected Zip files containing Microsoft Word documents appear to be experimental and it remains to be seen if they will be adopted for broader use.

Attachments

The following is a list of known types of email attachments used by TA542. All types of attachments are first-stage downloaders that attempt to download the Emotet payload or another intermediary downloader, as in the case of PDFs, from one of several (typically five) hardcoded payload URLs. Many unique attachments can contain the same set of payload URLs. TA542 also exchanges the URL sets several times a day.

- Microsoft Word documents with macros
- PDFs with links to Microsoft Word documents with macros
- PDFs with links to Zip archives with JScript files inside
- Password-protected Zip archives with JScript files inside

- Password-protected Zip files containing Microsoft Word documents

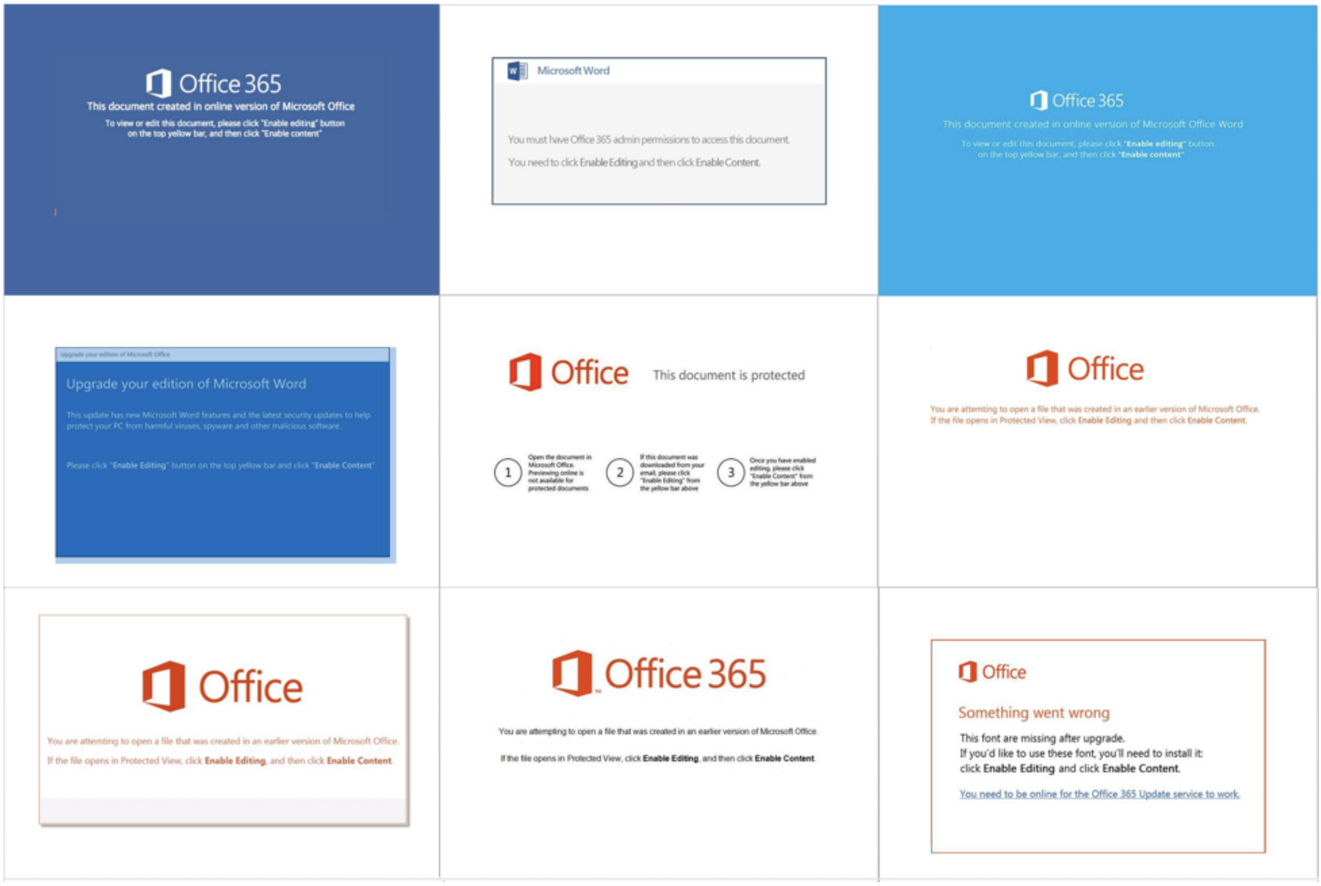
URLs

The following is a list of known types of URLs that the actor embeds in the emails. The URLs are frequently hosted on compromised vulnerable sites, including vulnerable WordPress installations. 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. The folder names are sometimes synchronized with the rest of the campaign theme, and might use stolen branding.

- URLs linking to Microsoft Word documents with macros
- URLs linking to Zipped Microsoft Word documents with macros
- URLs linking to Jscript
- URLs linking to Zipped JScript
- URLs linking to Zipped executables (not used since 2017)

Experiments

- April 3, 2019: First use of password-protected Zip files containing JScript. The actor has intermittently used this technique several more times.
- April 4, 2019: First use of password-protected Zip files containing Microsoft Word documents. At the time of writing of this analysis, the actor has only used this method once.



Office 365

This document created in online version of Microsoft Office

To view or edit this document, please click "Enable editing" button on the top yellow bar, and then click "Enable content"

Microsoft Word

You must have Office 365 admin permissions to access this document.

You need to click Enable Editing and then click Enable Content.

Office 365

This document created in online version of Microsoft Office Word

To view or edit this document, please click "**Enable editing**" button on the top yellow bar, and then click "**Enable content**"

Upgrade your edition of Microsoft Office

Upgrade your edition of Microsoft Word

This update has new Microsoft Word features and the latest security updates to help protect your PC from harmful viruses, spyware and other malicious software.

Please click "**Enable Editing**" button on the top yellow bar and click "**Enable Content**"

Office This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents
2. If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above
3. Once you have enabled editing, please click "Enable Content" from the yellow bar above

Office

You are attemting to open a file that was created in an earlier version of Microsoft Office. If the file opens in Protected View, click **Enable Editing** and then click **Enable Content**.

Office

You are attemting to open a file that was created in an earlier version of Microsoft Office.

If the file opens in Protected View, click **Enable Editing**, and then click **Enable Content**.

Office 365

You are attempting to open a file that was created in an earlier version of Microsoft Office.

If the file opens in Protected View, click **Enable Editing**, and then click **Enable Content**.

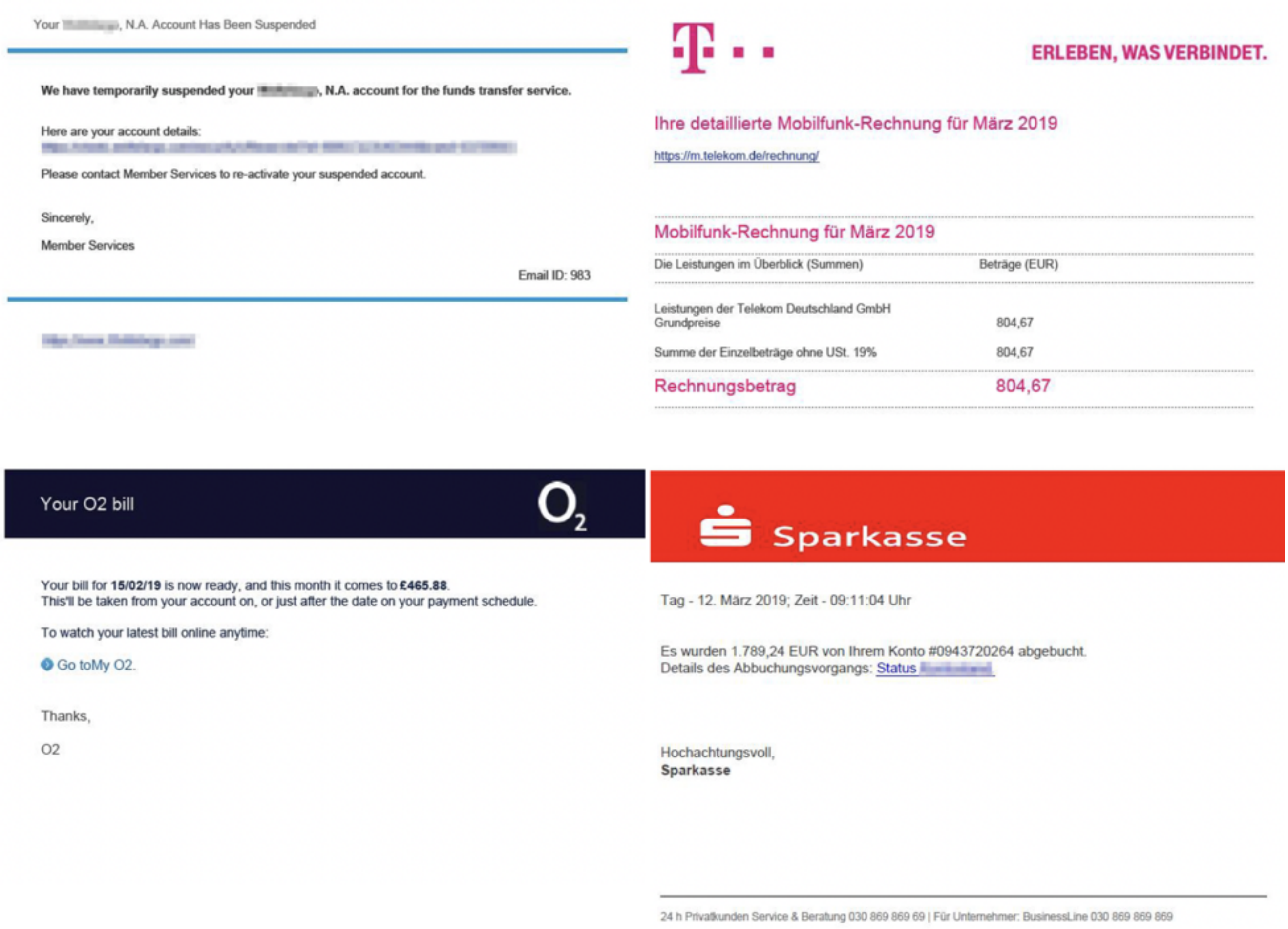
Office

Something went wrong

This font are missing after upgrade.
If you'd like to use these font, you'll need to install it:
click **Enable Editing** and click **Enable Content**.

You need to be online for the Office 365 Update service to work.

Figure 5: TA542 most commonly uses Microsoft Word documents with macros. The actor periodically updates the visual lure used in the document. This collage shows many of the lures used.



Your [redacted], N.A. Account Has Been Suspended

We have temporarily suspended your [redacted], N.A. account for the funds transfer service.

Here are your account details:
[redacted]
Please contact Member Services to re-activate your suspended account.

Sincerely,

Member Services

Email ID: 983

[redacted]

Ihre detaillierte Mobilfunk-Rechnung für März 2019

https://m.telekom.de/rechnung/

Mobilfunk-Rechnung für März 2019

Die Leistungen im Überblick (Summen)	Beträge (EUR)
Leistungen der Telekom Deutschland GmbH Grundpreise	804,67
Summe der Einzelbeträge ohne USt. 19%	804,67
Rechnungsbetrag	804,67

Your bill for **15/02/19** is now ready, and this month it comes to **£465.88**.
This'll be taken from your account on, or just after the date on your payment schedule.

To watch your latest bill online anytime:

Go toMy O2.

Thanks,

O2

Tag - 12. März 2019; Zeit - 09:11:04 Uhr

Es wurden 1.789,24 EUR von Ihrem Konto #0943720264 abgebucht.
Details des Abbuchungsvorgangs: Status [redacted]

Hochachtungsvoll,
Sparkasse

24 h Privatkunden Service & Beratung 030 869 869 69 | Für Unternehmer: BusinessLine 030 869 869 869

Figure 6: PDF attachment examples used by this threat actor. The actor commonly abuses branding of large financial institutions, telecommunications companies, and more in the PDFs

Conclusion

In the last two years, TA542 has become one of the most prolific threat actors in the overall threat landscape. Leveraging a robust Botnet known as Emotet, TA542 orchestrates high-volume, international email campaigns that distribute hundreds of thousands or even millions of messages per day. They use Emotet to download third-party banking malware such as The Trick, IcedID, and Gootkit, and to facilitate the continued spread of their botnet via a number of modules. As TA542 continues to operate at near-global scale, we can expect Emotet use to grow in the upcoming quarters.

References

[1] https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/

[2] https://web.archive.org/web/20140708121405/https://www.abuse.ch/?p=7930

[3] https://www.proofpoint.com/us/threat-insight/post/proofpoint-threat-report-banking-trojans-dominate-malware-landscape-first-months

[4] https://www.trendmicro.com/vinfo/nz/security/news/cybercrime-and-digital-threats/further-emotet-evolution-operators-hijacking-existing-email-threads-to-deliver-malware

[5] https://cofense.com/emotet-gang-switches-highly-customized-templates-utilizing-stolen-email-content-victims/

[6] https://www.kryptoslogic.com/blog/2018/10/emotet-awakens-with-new-campaign-of-mass-email-exfiltration/

[7] https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/

[8] https://www.cert.pl/en/news/single/analysis-of-emotet-v4/

[9] https://twitter.com/kafeine/status/804360636847321088

[10] https://www.fidelissecurity.com/threatgeek/threat-intelligence/emotet-network-spreader-component/

[11] https://www.gdata.de/blog/2017/10/30110-emotet-beutet-outlook-aus

Subscribe to the Proofpoint Blog