

# BazarBackdoor's Stealthy Infiltration Evades Multiple SEGs

---

[cofense.com/blog/bazarbackdoor-stealthy-infiltration](https://cofense.com/blog/bazarbackdoor-stealthy-infiltration)

Cofense

February 9, 2021

## Phish Found in Environments Protected by SEGs

---

### ProofPoint

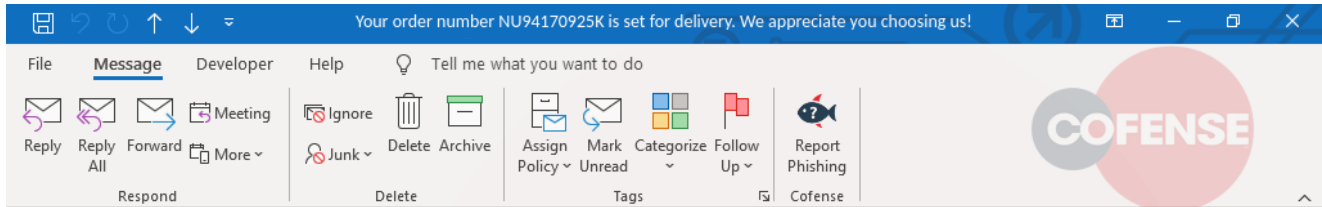
### Microsoft EOP

### Symantec

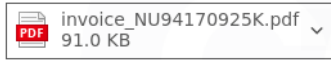
### Microsoft ATP

By Zachary Bailey, *Cofense Phishing Defense Center*

The Cofense PDC has been tracking a stealthy malware campaign that has recently become more active compromising enterprise endpoints. The campaign, first observed in mid-December, carries pharmaceutical-themed invoices that contain references to a series of websites hosted on the “shop” domain but that were down at the time of initial analysis. They were classified by the PDC as malicious because of the phone numbers used on the invoices. These numbers were identical across invoices being sent in from different brands and senders, which meant these are likely coordinated. The main lures of the emails also revolved around contacting the phone number instead of visiting the site.



Your order number NU94170925K is set for delivery. We appreciate you choosing us!



Dear customer,  
Thank you for using our services! Your order # NU94170925K Always yours, Top Tips Office!

All the information about your order is in the invoice  
Your order will be send to you in a shortest time, our managers already working on it!  
It will be shipped outtomorrow via FedEx, per your request.  
Due to the epidemiological situation, the delivery time may change.  
After the transfer of your request to the conveyance administration, you will get a SMS messagee with a track number.  
As soon as your order will be ready for delivery, you will be notified by our courier.  
We sincerely hope that you will enjoy your acquisition!

If you have any questions about your order or you decided to cancel it you can always contact us: +1 (831) 400 5370

Thank you for choosing Top Tips Office Store.

Sincerely,  
Top Tips Office

Figure 1: Email Body

New waves of the phishing emails are now being sent overnight with new brands ranging from office supplies, rose delivery and lingerie. After monitoring certain internet sources, PDC analysts were able to pull up the referenced sites while they were still live. Following an involved process of interacting with the site to request a cancellation form, a malicious Excel document was finally retrieved. This infection was the first stage of the BazarBackdoor malware.

The invoice ruse bypassed various customer SEGs because the email had no malicious payload and could be seen as a simple phishing scam. Only a handful of recipients would think to browse to the invoice site and search for a way to cancel their order without calling the number provided.



## Offices Supply

1407 Pacific Ave  
Santa Cruz, CA 95060  
1 (831) 480 4376  
officesupply.shop

**INVOICE NO.** [834572-00001329]  
**DATE** January 22, 2021

QTY	DESCRIPTION	UNIT PRICE	LINE TOTAL
1	Compatible Black Canon E40 Toner Cartridge (Replaces Canon 1491A002AA)	55.75	\$55.75

*Figure 2: Invoice Attachment*

While the invoices use a basic template, they look just professional enough that an inquisitive recipient might check the site to see if it's legitimate. Invoices for the older campaigns would be named after the order number, but recent campaigns are utilizing a "invoice\_\*.pdf" format, where the star (\*) wildcard is the order number.

Interested in high-fidelity phishing alerts and threat intelligence? Get a FREE 30-day trial of Cofense Intelligence.

### Get Your Free Access

It has been observed that the next stage in this social engineering attack alternates between being located on the contact, FAQ and refund pages of the website.

The image shows a contact form on a dark purple background. At the top left, there is a red envelope icon. To its right, the text reads: "If you change your mind about your purchase, you have the option to modify or cancel it." Below this, it says: "To modify or cancel your order, please follow the steps below". In the top right corner, there is a circular logo with the word "COFENSE" inside. Below the text, there is a label "Order number \*" followed by a white input field containing the placeholder text "Input your order number". At the bottom left of the form, there is a white "Submit" button.

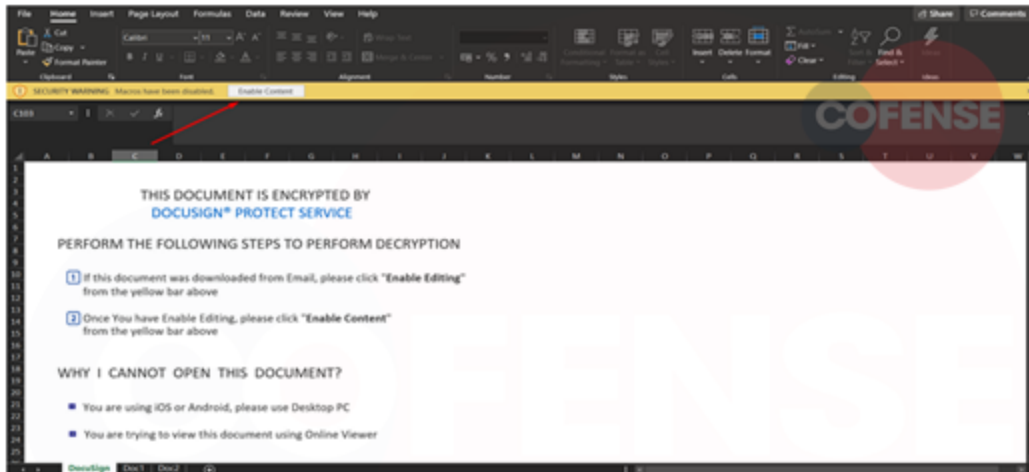
*Figure 3: Contact Form*

If the order number is entered, the recipient will be transferred to a new website with a “.us” domain version of the prior website. There are several variations of the site, for instance using hyphens to break up the words or using only the first and third words of the fictitious brand. Examples of this would be compact-ssd[.]us and compactstorage[.]us.

**Order status: processed**

Your order is being processed at 01.26.2021. 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.**



**Only for Google Chrome users**

**Help**

**The form could be downloaded here:**

[Request Form](#)

**Send the filled out form to this [email](#)**

*Figure 4: Download Page*

Once the site is loaded, a series of images walks the user through downloading a form to cancel their order. There is a link to the request form, and a link to an email where the form is to be sent. This furthers the ruse’s legitimacy. The downloaded form is an Excel document that appears to be encrypted by DocuSign.

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

Figure 5: Excel Template

This Excel template is themed similarly to a Trickbot template reported on Twitter by [@ffforward](#), who has been tracking the campaign closely. This connection makes sense considering the agreement in many quarters that there is a connection between Trickbot operators and the group behind BazarBackdoor.

When the form is activated, an .EXE payload is immediately launched. This executable is also a new variant of BazarBackdoor. It will reload itself into memory several times before the command-and-controls (C2s) can finally be extracted. Next, the executable queries the geographical location and IP address of the infected machine. This is a common tactic that usually ensures that the threat actor does not infect machines in their country of operation.

Address	Length	Result
0x3923eff6b0	76	cegiikdeiiin.bazar bceikkccgikn.bazar begiklceiiko.bazar deehimeeghip.bazar
0x3923eff754	76	cegiikdeiiin.bazar bceikkccgikn.bazar begiklceiiko.bazar deehimeeghip.bazar
0x1f632205b90	18	cegiikdeiiin.bazar

Figure 6: Bazar in Memory Strings

After the .EXE finishes loading, we see BazarBackdoor domains in the memory strings.

9 results.

Address	Length	Result
0x1f6321dfa80	88	https://192.168.0.1/organization/round_table
0x1f6321dfb60	88	https://192.168.0.1/organization/round_table
0x1f6321dfbd0	94	https://34.220.167.220/organization/round_table
0x1f6321dfd20	94	https://34.220.167.220/organization/round_table
0x1f6321dfee0	92	https://54.190.50.234/organization/round_table
0x1f6321dff0	92	https://54.190.50.234/organization/round_table
0x1f6321f87f0	50	/organization/round_table
0x1f6321f88f0	50	/organization/round_table
0x1f6321f8d30	50	/organization/round_table

Figure 7: C2s for Bazarbackdoor

We also can find this campaign's C2 for dropping the next stage by searching for IP addresses in the strings. There is often a common word in the C2s, such as "cleaner" or "book" or "snow" that differentiates between campaigns. In the observed campaign for this article, that word is "round\_table".




















 UDP Send	192.168.18.200:60404 -> 51.254.25.115:53
 UDP Send	192.168.18.200:60405 -> 193.183.98.66:53
 UDP Send	192.168.18.200:60406 -> 91.217.137.37:53
 UDP Send	192.168.18.200:60407 -> 87.98.175.85:53
 UDP Send	192.168.18.200:60408 -> 185.121.177.177:53
 UDP Send	192.168.18.200:60409 -> 169.239.202.202:53
 UDP Send	192.168.18.200:60410 -> 198.251.90.143:53
 UDP Send	192.168.18.200:60411 -> 5.132.191.104:53
 UDP Send	192.168.18.200:60412 -> 111.67.20.8:53
 UDP Send	192.168.18.200:60413 -> 163.53.248.170:53
 UDP Send	192.168.18.200:60414 -> 142.4.204.111:53
 UDP Send	192.168.18.200:60415 -> 142.4.205.47:53
 UDP Send	192.168.18.200:60416 -> 158.69.239.167:53
 UDP Send	192.168.18.200:60417 -> 104.37.195.178:53
 UDP Send	192.168.18.200:60418 -> 192.99.85.244:53
 UDP Send	192.168.18.200:60419 -> 158.69.160.164:53
 UDP Send	192.168.18.200:60420 -> 46.28.207.199:53
 UDP Send	192.168.18.200:60421 -> 31.171.251.118:53
 UDP Send	192.168.18.200:60422 -> 81.2.241.148:53

Figure 8: DNS traffic

An analysis of the machine's network traffic reveals that DNS requests are being sent by BazarBackdoor. This is a common technique the malware employs to mask the servers behind the "bazar" domains. The TCP connections to the three "round\_table" servers will drop a data file that is likely part of the next stage.

Recent invoice templates have shifted from using the ".shop" domain to ".net" domains. This campaign was also referred to as "BazarCall" by @ffforward. It is widely believed that this campaign, like prior BazarBackdoor campaigns, will distribute Ryuk ransomware across the network. An analysis by [The DFIR Report](#) found Cobalt strike beacons in their environment, and PowerShell scripts that are seen in conjunction with Ryuk. However, no Ryuk was deployed during the analysis.

The Cofense PDC is still looking into the connection between Kontakt Kegtap and the Bazarloader/Bazarbackdoor campaigns being delivered from Google Docs and GetResponse.

## Indicators of Compromise

<b>Domain</b>	<b>IP</b>
hxxp://flowersny[.]net/	104[.]21[.]7[.]245
hxxp://flowersny[.]us/	104[.]21[.]23[.]158
hxxp://ttooffice[.]net/	104[.]21[.]84[.]40
hxxp://ttooffice[.]us	162[.]255[.]119[.]138
hxxp://toptipsoffice[.]us	194[.]147[.]115[.]9
hxxp://ajourlingerie[.]net	104[.]21[.]8[.]207
hxxp://ajourlingerie[.]us/	104[.]21[.]4[.]188

<b>Command and Control URLs</b>	<b>IP</b>
hxxps://18[.]188[.]232[.]155:443/leading/crisis26/snow11	18[.]188[.]232[.]155
hxxps://18[.]191[.]220[.]165/leading/crisis26/snow11	18[.]191[.]220[.]165
hxxps://54[.]190[.]50[.]234/organization/round_table	4[.]190[.]50[.]234

hxxps://54[.]215[.]217[.]171/	54[.]215[.]217[.]171
hxxps://34[.]209[.]41[.]233/foreground/suspect/context59	34[.]209[.]41[.]233
hxxps://34[.]220[.]167[.]220/organization/round_table	34[.]220[.]167[.]220
hxxps://34[.]221[.]125[.]90/foreground/suspect/context59	34[.]221[.]125[.]90
hxxps://japort[.]com/suret/victory[.]php	50[.]87[.]232[.]245

DNS IOCs	IP
51[.]254[.]25[.]115:53	51[.]254[.]25[.]115
193[.]183[.]98[.]66:53	193[.]183[.]98[.]66
91[.]217[.]137[.]37:53	91[.]217[.]137[.]37
87[.]98[.]175[.]85:53	87[.]98[.]175[.]85
185[.]121[.]177[.]177:53	185[.]121[.]177[.]177
169[.]239[.]202[.]202:53	169[.]239[.]202[.]202
198[.]251[.]90[.]143:53	198[.]251[.]90[.]143
5[.]132[.]191[.]104:53	5[.]132[.]191[.]104
111[.]67[.]20[.]8:53	111[.]67[.]20[.]8
163[.]53[.]248[.]170:53	163[.]53[.]248[.]170
142[.]4[.]204[.]111:53	142[.]4[.]204[.]111
142[.]4[.]205[.]47:53	142[.]4[.]205[.]47
158[.]69[.]239[.]167:53	158[.]69[.]239[.]167
104[.]37[.]195[.]178:53	104[.]37[.]195[.]178
192[.]99[.]85[.]244:53	192[.]99[.]85[.]244
158[.]69[.]160[.]164:53	158[.]69[.]160[.]164
46[.]28[.]207[.]199:53	46[.]28[.]207[.]199



31[.]171[.]251[.]118:53	31[.]171[.]251[.]118
81[.]2[.]241[.]148:53	81[.]2[.]241[.]148
82[.]141[.]39[.]32:53	82[.]141[.]39[.]32
50[.]3[.]82[.]215:53	50[.]3[.]82[.]215
46[.]101[.]70[.]183:53	46[.]101[.]70[.]183
5[.]45[.]97[.]127:53	5[.]45[.]97[.]127
130[.]255[.]78[.]223:53	130[.]255[.]78[.]223
144[.]76[.]133[.]38:53	144[.]76[.]133[.]38
139[.]59[.]208[.]246:53	139[.]59[.]208[.]246
172[.]104[.]136[.]243:53	172[.]104[.]136[.]243
45[.]71[.]112[.]70:53	45[.]71[.]112[.]70
163[.]172[.]185[.]51:53	163[.]172[.]185[.]51
5[.]135[.]183[.]146:53	5[.]135[.]183[.]146
51[.]255[.]48[.]78:53	51[.]255[.]48[.]78
188[.]165[.]200[.]156:53	188[.]165[.]200[.]156
147[.]135[.]185[.]78:53	147[.]135[.]185[.]78
92[.]222[.]97[.]145:53	92[.]222[.]97[.]145
51[.]255[.]211[.]146:53	51[.]255[.]211[.]146
159[.]89[.]249[.]249:53	159[.]89[.]249[.]249
104[.]238[.]186[.]189:53	104[.]238[.]186[.]189
139[.]59[.]23[.]241:53	139[.]59[.]23[.]241
94[.]177[.]171[.]127:53	94[.]177[.]171[.]127
45[.]63[.]124[.]65:53	45[.]63[.]124[.]65
212[.]24[.]98[.]54:53	212[.]24[.]98[.]54
178[.]17[.]170[.]179:53	178[.]17[.]170[.]179
185[.]208[.]208[.]141:53	185[.]208[.]208[.]141

82[.]196[.]9[.]45:53	82[.]196[.]9[.]45
146[.]185[.]176[.]36:53	146[.]185[.]176[.]36
89[.]35[.]39[.]64:53	89[.]35[.]39[.]64
89[.]18[.]27[.]167:53	89[.]18[.]27[.]167
77[.]73[.]68[.]161:53	77[.]73[.]68[.]161
185[.]117[.]154[.]144:53	185[.]117[.]154[.]144
176[.]126[.]70[.]119:53	176[.]126[.]70[.]119
139[.]99[.]96[.]146:53	139[.]99[.]96[.]146
217[.]12[.]210[.]54:53	217[.]12[.]210[.]54
185[.]164[.]136[.]225:53	185[.]164[.]136[.]225
192[.]52[.]166[.]110:53	192[.]52[.]166[.]110
63[.]231[.]92[.]27:53	63[.]231[.]92[.]27
66[.]70[.]211[.]246:53	66[.]70[.]211[.]246
96[.]47[.]228[.]108:53	96[.]47[.]228[.]108
45[.]32[.]160[.]206:53	45[.]32[.]160[.]206
128[.]52[.]130[.]209:53	128[.]52[.]130[.]209
35[.]196[.]105[.]24:53	35[.]196[.]105[.]24
172[.]98[.]193[.]42:53	172[.]98[.]193[.]42
162[.]248[.]241[.]94:53	162[.]248[.]241[.]94
107[.]172[.]42[.]186:53	107[.]172[.]42[.]186
167[.]99[.]153[.]82:53	167[.]99[.]153[.]82
138[.]197[.]25[.]214:53	138[.]197[.]25[.]214
69[.]164[.]196[.]21:53	69[.]164[.]196[.]21
192[.]71[.]245[.]208:53	192[.]71[.]245[.]208
185[.]120[.]22[.]15:53	185[.]120[.]22[.]15
45[.]71[.]185[.]100:53	45[.]71[.]185[.]100

***All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats.***

***The Cofense® and PhishMe® names and logos, as well as any other Cofense product or service names or logos displayed on this blog are registered trademarks or trademarks of Cofense Inc.***

Don't miss out on any of our phishing updates! Subscribe to our blog.