THREAT BULLETINS

UPDATE: BazaCall Campaign Targets Healthcare Entities

TLP:WHITE

Jul 30, 2021

Microsoft has published BazaCall: Phony Call Centers Lead to Exfiltration and Ransomware**,** detailing new insights derived from their continued investigation into BazaCall campaigns.

The **BazaCall** campaigns use emails that instruct recipients to call a number to cancel their supposed subscription to a service. When victims call the number, they reach a fraudulent call center operated by attackers who tell them to visit a website and download an Excel file to cancel the service. This file contains a malicious macro that downloads the payload.

When the Excel macros are enabled, the **BazaCall** malware will be downloaded and executed on the victim's computer, which then deploys **ransomware**.

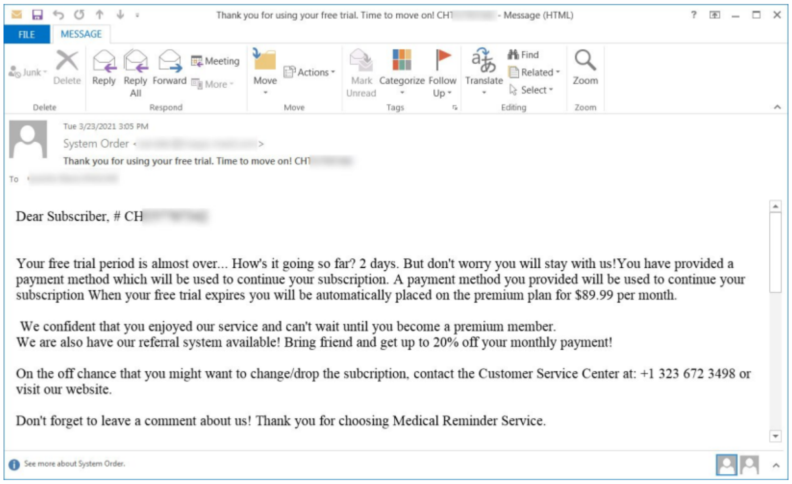
This campaign is named after **BazaLoader**, the malware it initially distributed. The malware is designed to provide backdoor access to an infected Windows device. Attackers can then send other forms of malware, scan the target environment, and go after other vulnerable machines on the same network. The group behind **BazaLoader** uses different methods to distribute its malware.

Please review the Microsoft Security Blog post for additional insight.

While this is not the first time cybercrime gangs have worked together with underground call centers, this is the first time we have seen a major malware distributor, such as the BazarLoader gang, use this tactic on a large scale.

Like many malware campaigns, BazaCall starts with a phishing email but from there deviates to a novel distribution method; using phone call centers to distribute malicious Excel documents that install malware.

The emails then prompt the user to contact a listed phone number to cancel the subscription before they are charged $69.99 to $89.99 for a renewal, as shown in the example BazaCall phishing email below.



Thank you for using your free trial. Time to move on! CH[redacted] - Message (HTML)

Tue 3/23/2021 3:05 PM
System Order <[redacted]>
Thank you for using your free trial. Time to move on! CH[redacted]
To [redacted]

Dear Subscriber, # CH[redacted]

Your free trial period is almost over... How's it going so far? 2 days. But don't worry you will stay with us!You have provided a payment method which will be used to continue your subscription. A payment method you provided will be used to continue your subscription When your free trial expires you will be automatically placed on the premium plan for $89.99 per month.

We confident that you enjoyed our service and can't wait until you become a premium member.
We are also have our referral system available! Bring friend and get up to 20% off your monthly payment!

On the off chance that you might want to change/drop the subcription, contact the Customer Service Center at: +1 323 672 3498 or visit our website.

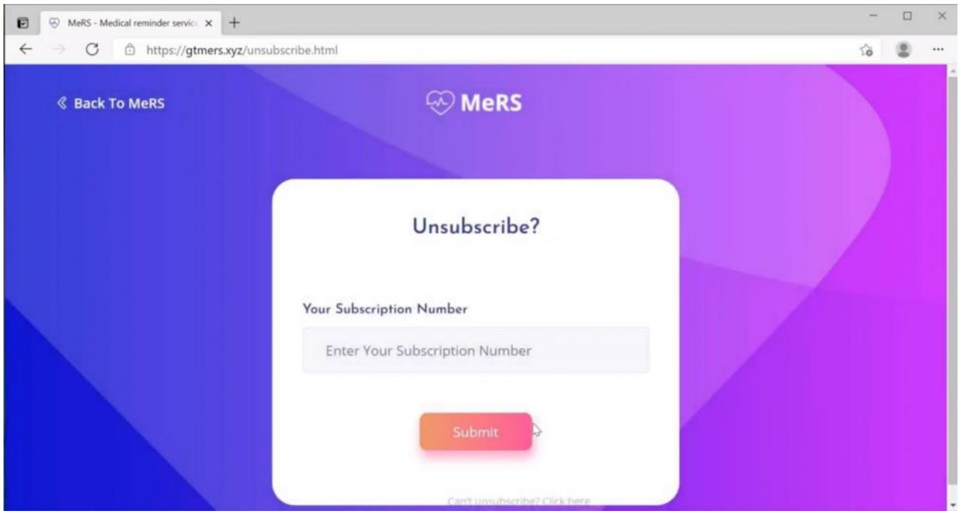
Don't forget to leave a comment about us! Thank you for choosing Medical Reminder Service.

See more about System Order.

When a recipient calls the listed phone number, they will be placed on a short hold and then greeted by a live person.

When asked for more information or how to cancel the subscription, the call center agent asks the victim for a unique customer ID enclosed in the email.

If a correct customer ID is given, the call center agent will direct the user to a malicious website that purports to be the associated medical services company. The phone agent will stay on the phone with the victim and guide them to a cancellation page where they are prompted to enter their customer ID, as shown below.


MeRS - Medical reminder servic
https://gtmers.xyz/unsubscribe.html
Back To MeRS
MeRS
Unsubscribe?
Your Subscription Number
Enter Your Subscription Number
Submit
Can't unsubscribe? Click here

When the user enters their correct customer ID number, the website will automatically prompt the browser to download an Excel document, either xls or xlsb. The call center agent will then help the victim open the file by instructing the victim to click on the 'Enable Content' button to enable malicious macros.

When the Excel macros are enabled, the BazaCall malware will be downloaded and executed on the victim's computer, which then deploys ransomware.

Indicators of Compromise:

The following indicators have already been ingested into the Health-ISAC automated threat feed.

Email Addresses:

- info[@]icartservice.com
- inform[@]icartservice.com

- it[@]icartservice.com

Subjects:

- Do you want to extend your free period ###########?
- Do you want to extend your free trial ###########?
- Free period for ############ will come to the end end in 3 days
- Free trial period for ############ ends in three days
- Free trial period for ############ will end in 3 days
- Your free period ########### is about to end!
- Your free trial ########### is about to end!

Maldoc Download URLS:

- hxxps[:]//buyimers.us/unsubscribe.html
- hxxps[:]//geticart.us/unsubscribe.html
- hxxps[:]//getmers.us/unsubscribe.html
- hxxps[:]//gobcs.us/unsubscribe.html
- hxxps[:]//goimed.us/unsubscribe.html
- Buyimers[.]us
- Geticart[.]us
- Getmers[.]us
- Gobcs[.]us
- Goimed[.]us

Maldoc (XLSB) File Hashes:

- 09740a9d5d1b3d09d64d22d019567784
- 1974d98db0e8867165b008f7c46404a1
- 5a8f6aa70fae15ba88c0c159c30f923d
- cdd3aacf99acd2a4e339914c480a6afd

Payload Downloads URLS:

- hxxp[:]//beauty1.xyz/campo/l/l1

Additional Payload File Hashes:

- 1163[.]pk9
  - dd6cdec2609c165cc64b3bc22be5fe20
- 1163[.]ph5
  - 99bfec83b97bd216e06117c6468b19db
- 1163[.]xlsb
  - 99bfec83b97bd216e06117c6468b19db

Reference(s)	Microsoft

Recommendations

- Verify web links do not have misspellings or contain the wrong domain.
- Be suspicious of unsolicited phone calls, visits, or email messages from unknown individuals claiming to be from a legitimate organization. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. If possible, try to verify the caller's identity directly with the company.
- If you receive a vishing call, document the phone number of the caller as well as the domain that the actor tried to send you to and relay this information to law enforcement.
- Health-ISAC recommends appropriate user security awareness according to organizational policy, to include the possibility of applicable internal phishing exercises.

Sources

Bleeping Computer: Bazarcall Malware Uses Malicious Call Centers to Infect Victims

Hiemdal Security: New ‘BazarCall’ Malware Uses Call Centers to Trick its Victims into Infecting Themselves

Execute Malware: BazarCall IOCs
BAZARLOADER SCAM TARGETS VICTIMS WITH PHONY CALL CENTER EMAILS

Microsoft Tracks New BazaCall Malware Campaign
How legitimate security tool Cobalt Strike is being used in cyberattacks
BazaCall: Phony Call Centers Lead to Exfiltration and Ransomware

Alert ID 390b41fa

View Alert

Tags BazaCall

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.