Sophos 的研究人员发现了一个持续超过一年半且不断扩大和演变的欺诈团伙，利用虚假的移动应用程序来引诱受害者参与投资，精心构建骗局获取受害者的信任。

攻击者正在从华语受众人群转移到更普遍的范围，而不是局限于在亚洲。近期也发现诈骗团伙开始将虚假应用程序发布到 Apple Strore
上，尽力绕过苹果严格的审核机制。

研究人员调查了两个杀猪盘：

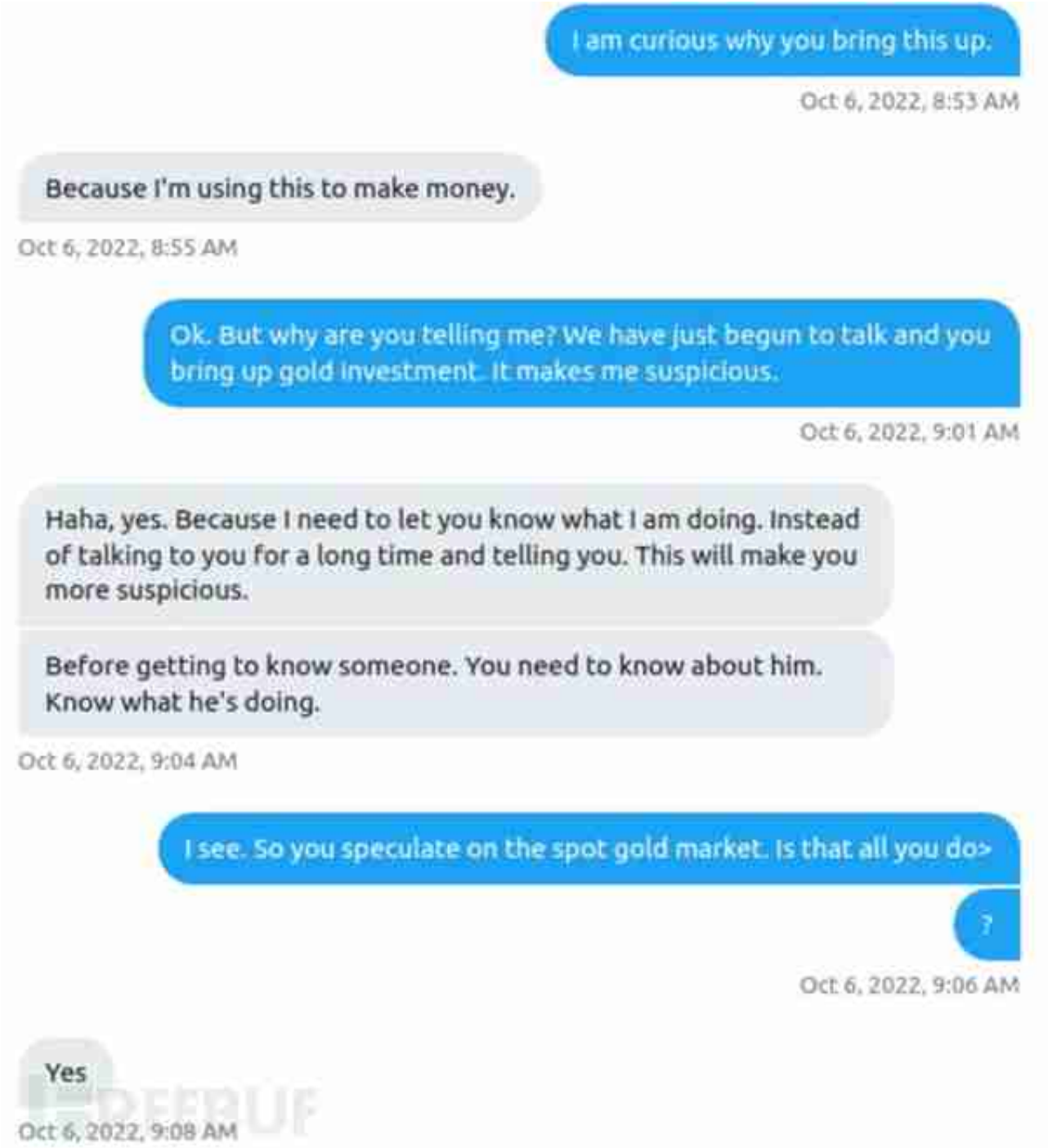
> 基于 MetaTrader 4
> 应用程序，运营一个虚假的黄金交易市场。诈骗团伙提供了
> Windows、Android 与 iOS
> 版本的应用程序，要求受害者上传大量个人身份信息，再引诱其汇款。
>
> 总部位于柬埔寨的诈骗团伙利用 TradingView
> 运营一个虚假的加密货币交易市场。诈骗团伙提供 Andorid 与 iOS
> 版本的应用程序，一个月内窃取了超过五十万美元的加密货币。

引你上钩

首先要和诈骗团伙连上线，直接通过 Twitter
联系骗子就可以。可以看到回复骗子之前，已经晾着骗子接近一个月的时间。

骗子的主页

研究人员表示自己研究网络安全领域的威胁，也调查诈骗。骗子在确认研究人员不是警察后，快速将话题转向了投资，介绍起黄金交易。



Twitter 交流

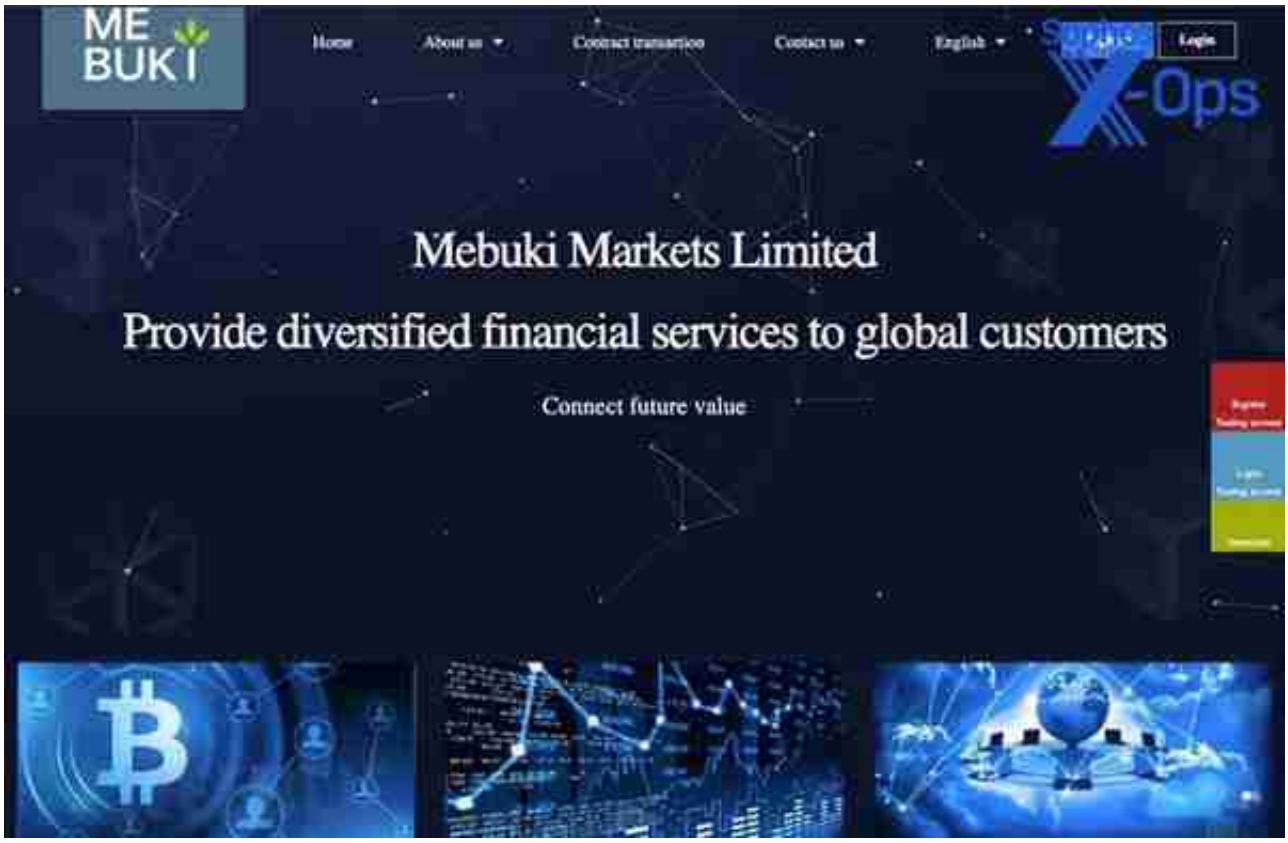
研究人员搁置了对话几天，但骗子仍然在持续发送消息。


Chen Zimo
last seen 6 hours ago
October 10
Hallo 03:16 PM
Oh hello. 03:16 PM
I am Chen Zimo. 03:16 PM
I see. 03:17 PM
So why did you want to move our conversation here? 03:17 PM
And why did your profile picture change? 03:18 PM
This is the Twitter that I use at work. 03:19 PM
I don't often use Twitter. 03:19 PM
ok 03:19 PM
How was your day? 03:19 PM
It is only halfway through. 03:21 PM
Are you halfway through your work? Or what's halfway through? 03:22 PM
Sophos X-Ops

Telegram 交流

Telegram 交流

研究人员询问了交易平台的情况，骗子给出了一个名称。经过搜索，可以找到模拟合法交易网站的诈骗网站。骗子还在外汇交易讨论网站上发布虚假评论，以宣传该诈骗网站。



诈骗网站

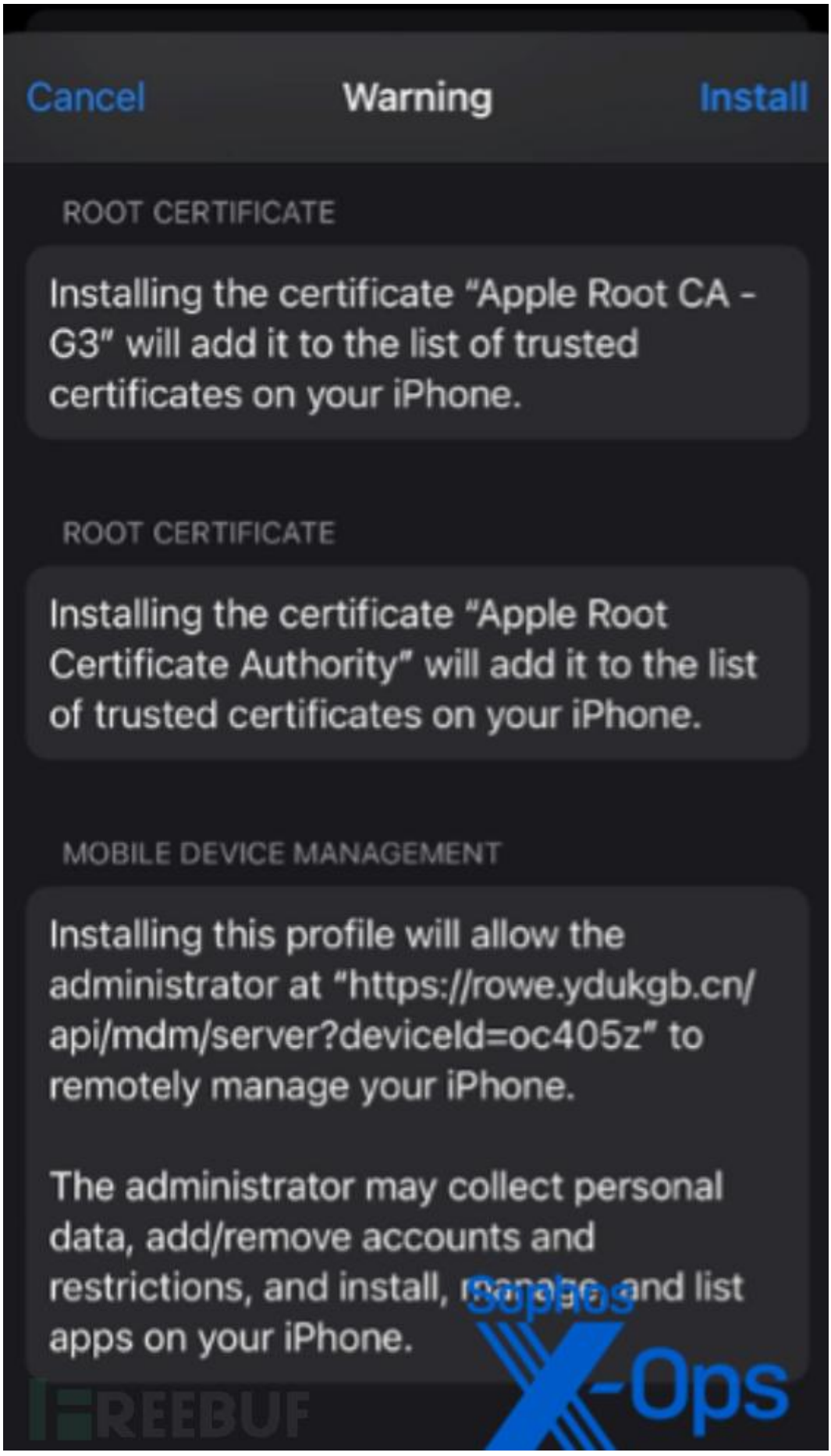
根据调查，主机上相关的多个网站几乎完全相同。这些网站都是诈骗网站，但是冒充的合法公司不同。

诈骗网站

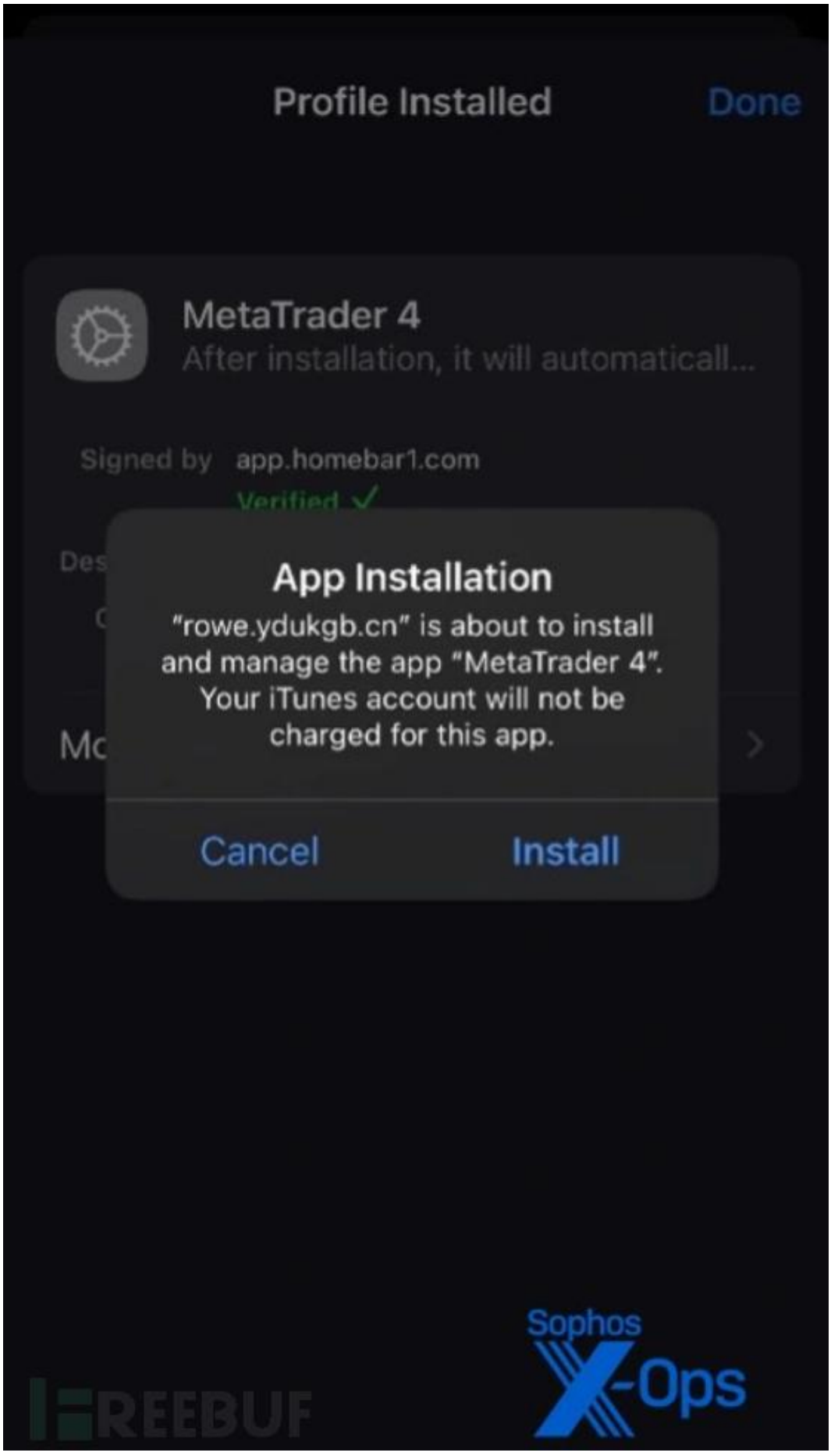
通过诈骗网站下载了应用程序后，研究人员再次表达了对网站的担忧：“为什么服务器部署在香港？为什么没有和实际公司在相同的国家？”

Telegram 交流

根据调查，骗子唯一说的实话就是她本人真的位于中国香港。骗子后续还向研究人员介绍了有关白银交易等虚假信息，研究人员来者不拒表示很感兴趣。

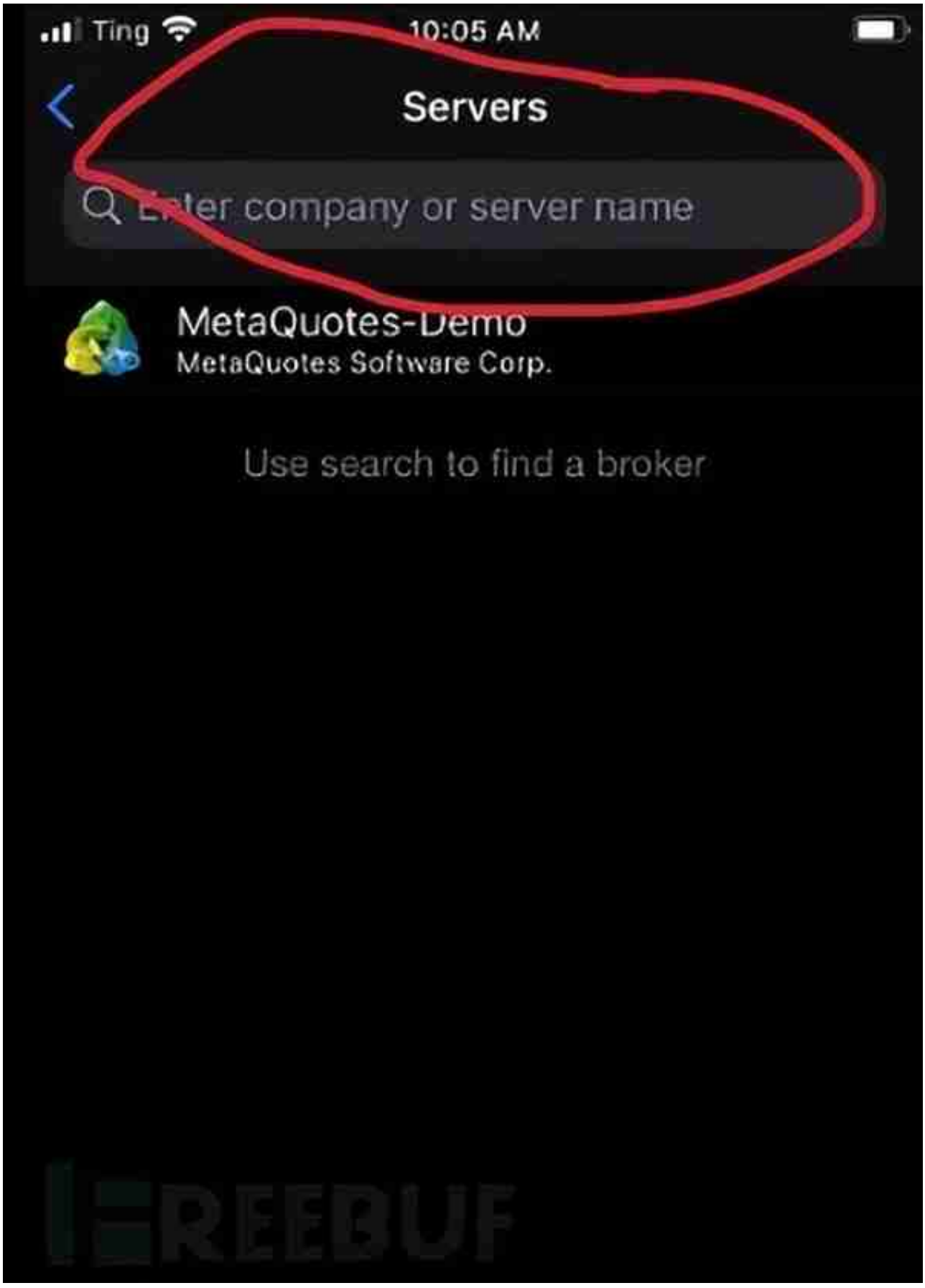

Cancel
Warning
Install
ROOT CERTIFICATE
Installing the certificate "Apple Root CA - G3" will add it to the list of trusted certificates on your iPhone.
ROOT CERTIFICATE
Installing the certificate "Apple Root Certificate Authority" will add it to the list of trusted certificates on your iPhone.
MOBILE DEVICE MANAGEMENT
Installing this profile will allow the administrator at "https://rowe.ydukgb.cn/api/mdm/server?deviceId=oc405z" to remotely manage your iPhone.
The administrator may collect personal data, add/remove accounts and restrictions, and install, manage, and list apps on your iPhone.
FREEBUF
Sophos
X-Ops

iOS 平台安装虚假应用程序


Profile Installed
Done
MetaTrader 4
After installation, it will automaticall...
Signed by app.homebar1.com
Verified
App Installation
"rowe.ydukgb.cn" is about to install and manage the app "MetaTrader 4". Your iTunes account will not be charged for this app.
Cancel
Install
Sophos
X-Ops
FREEBUF

iOS 平台安装虚假应用程序

研究人员问及为什么必须这样下载应用程序时，骗子表示这是由于被美国制裁。

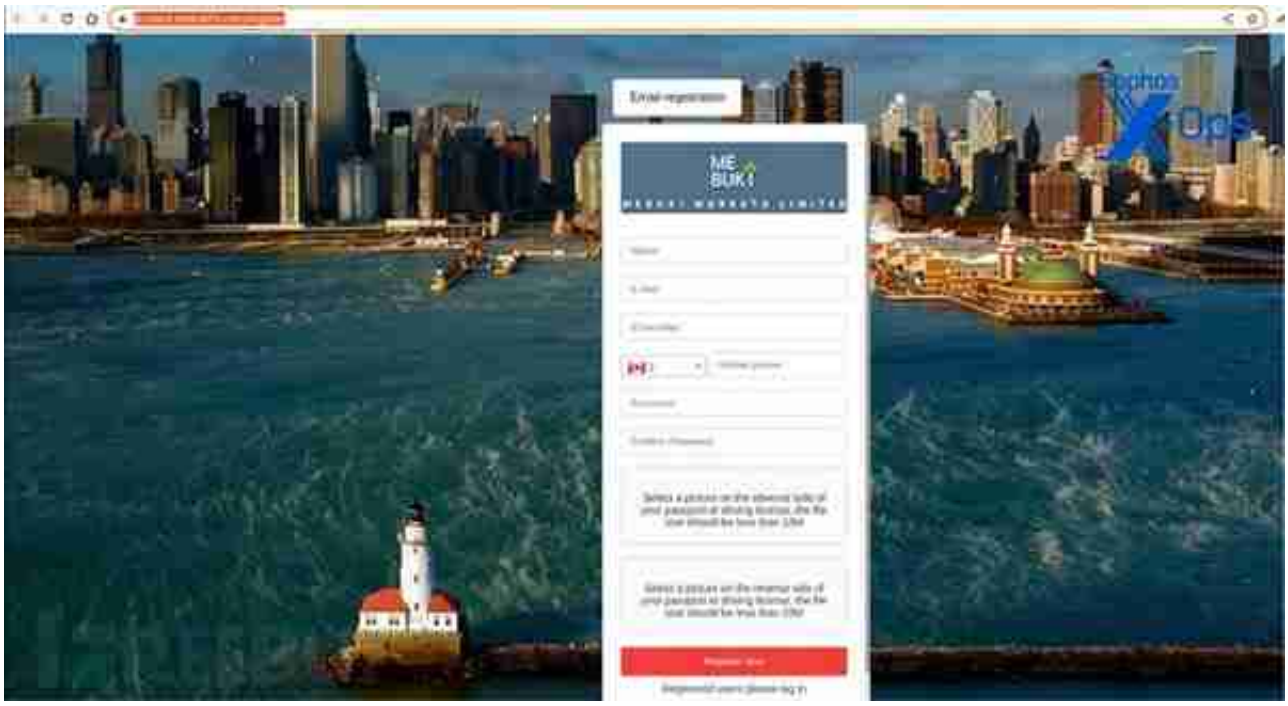

Ting
10:05 AM
Servers
Enter company or server name
MetaQuotes-Demo
MetaQuotes Software Corp.
Use search to find a broker
FREEBUF

配置指引

成功后，系统为用户设置一个余额为 10 万美元的练习账户。并且提供一个市场跟踪显示，由中国香港的另一个服务器提供的数据。

Telegram 交流

“叔叔”要求通过诈骗网站注册账户，提供相关信息。



柬埔寨诈骗团伙披露的照片

另外一个调查的柬埔寨诈骗团伙则更高级，构建了更复杂的背景故事。骗子会通过各种方法来建立信任关系，不过最终都是为了骗钱。

IOC

all.rcufgmj.cn.w.kunlunea.com
mebukiltd.com
account.mebukiltd.com
mt.mataquotes.com
mebukifx.com
account.mebukifx.com
spreades.com
billionmt4s.com
tickml.com
exness-eur.net
tosal-fx.com
app.homebar1.com
rowe.ydukgb.cn
spreades.com

参考来源

Sophos