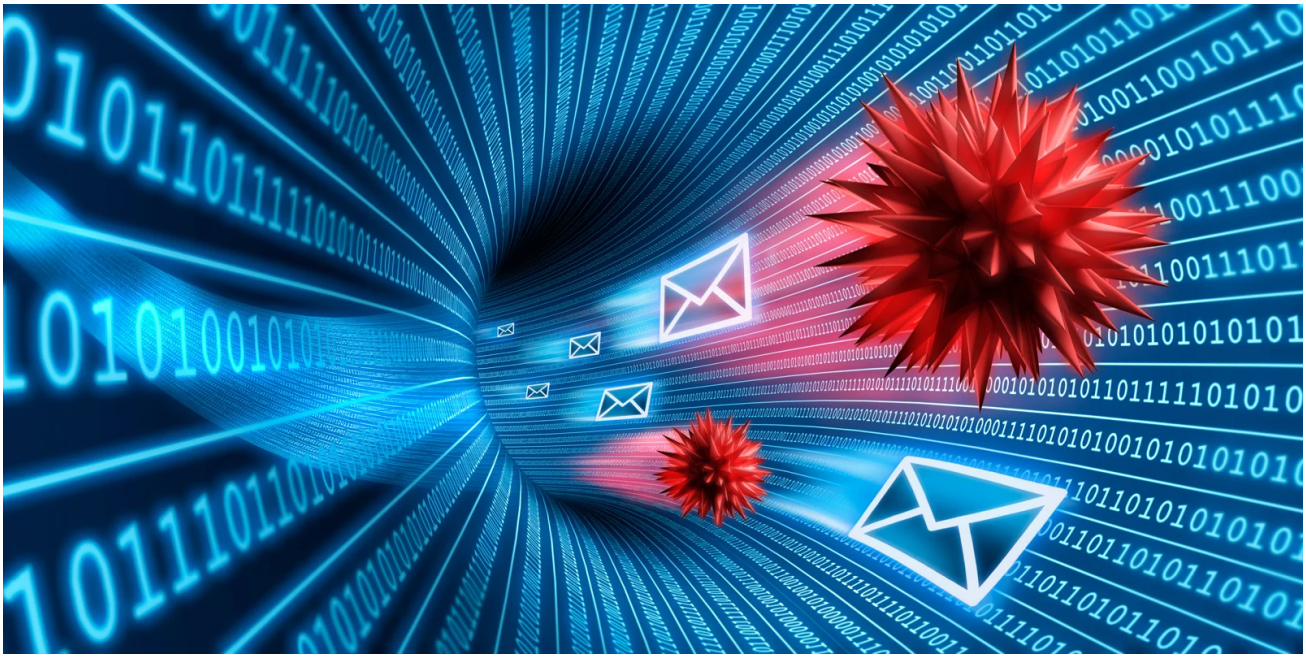
Malware campaign impersonates VC firm looking to buy sites

bleepingcomputer.com/news/security/malware-campaign-impersonates-vc-firm-looking-to-buy-sites/

Lawrence Abrams

By
Lawrence Abrams

- March 3, 2022
- 05:37 PM
- 0



BleepingComputer was recently contacted by an alleged "venture capitalist" firm that wanted to invest or purchase our site. However, as we later discovered, this was a malicious campaign designed to install malware that provides remote access to our devices.

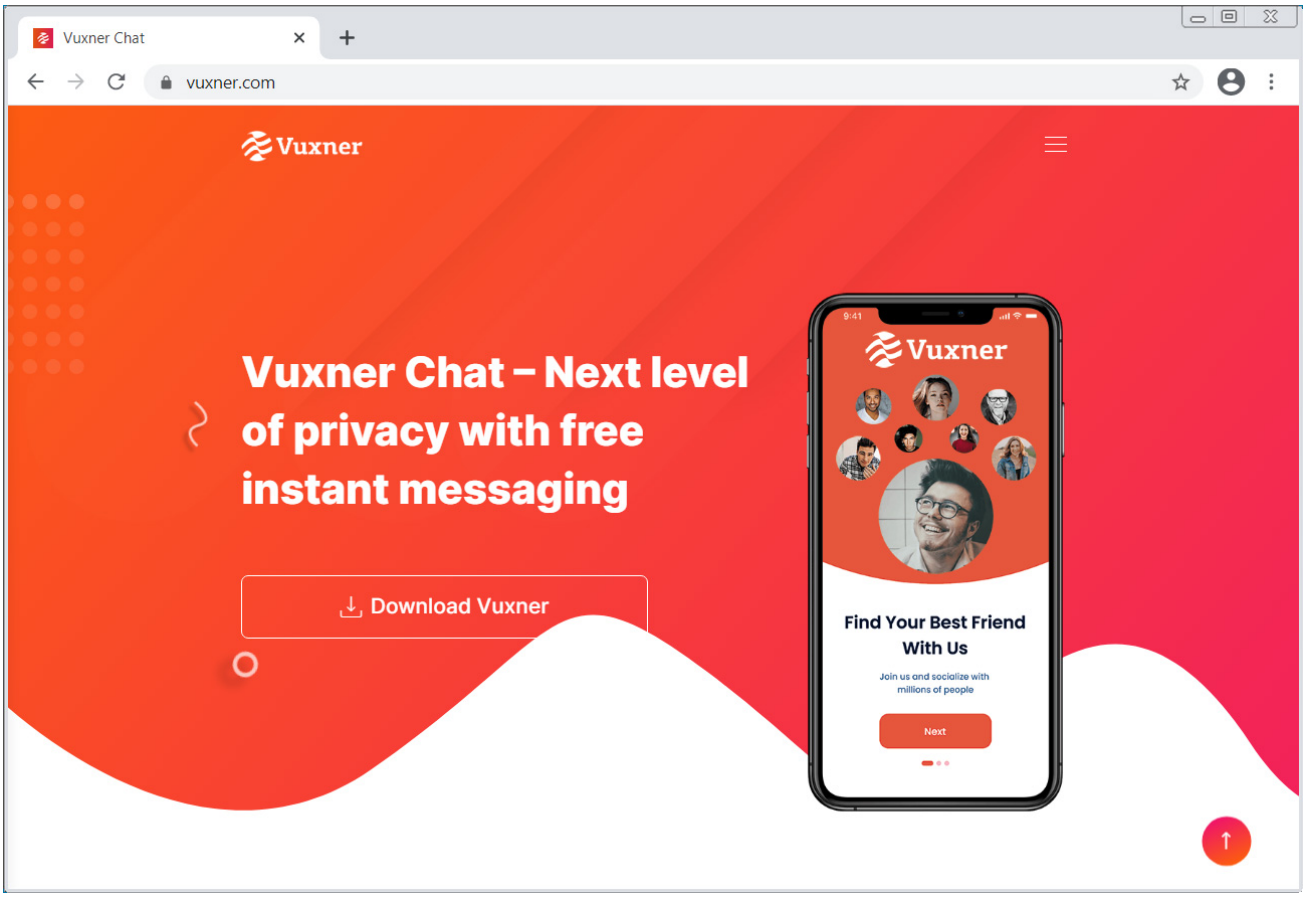
Last week, BleepingComputer received an email to our contact form from an IP address belonging to a United Kingdom virtual server company.

This email pretended to be from a venture capitalist interested in investing or buying BleepingComputer, with the whole email listed below.

> "Hello, we are a group of venture capitalists investing in promising projects.
> We saw your website and were astounded by your product. We want to discuss the opportunity to invest or buy a part of the share in your project. Please get in touch with us by phone or in Vuxner chat.
> Your agent is Philip Bennett. His username in Vuxner is philipbennett Make sure you contact us ASAP because we are not usually so generous with our offers. Thank you in advance!"

Writing about cybersecurity for so long, I am paranoid regarding email, messaging, and visiting unknown websites. So, I immediately grew suspicious of the email, fired up a virtual machine and VPN, and did a search for Vuxner.

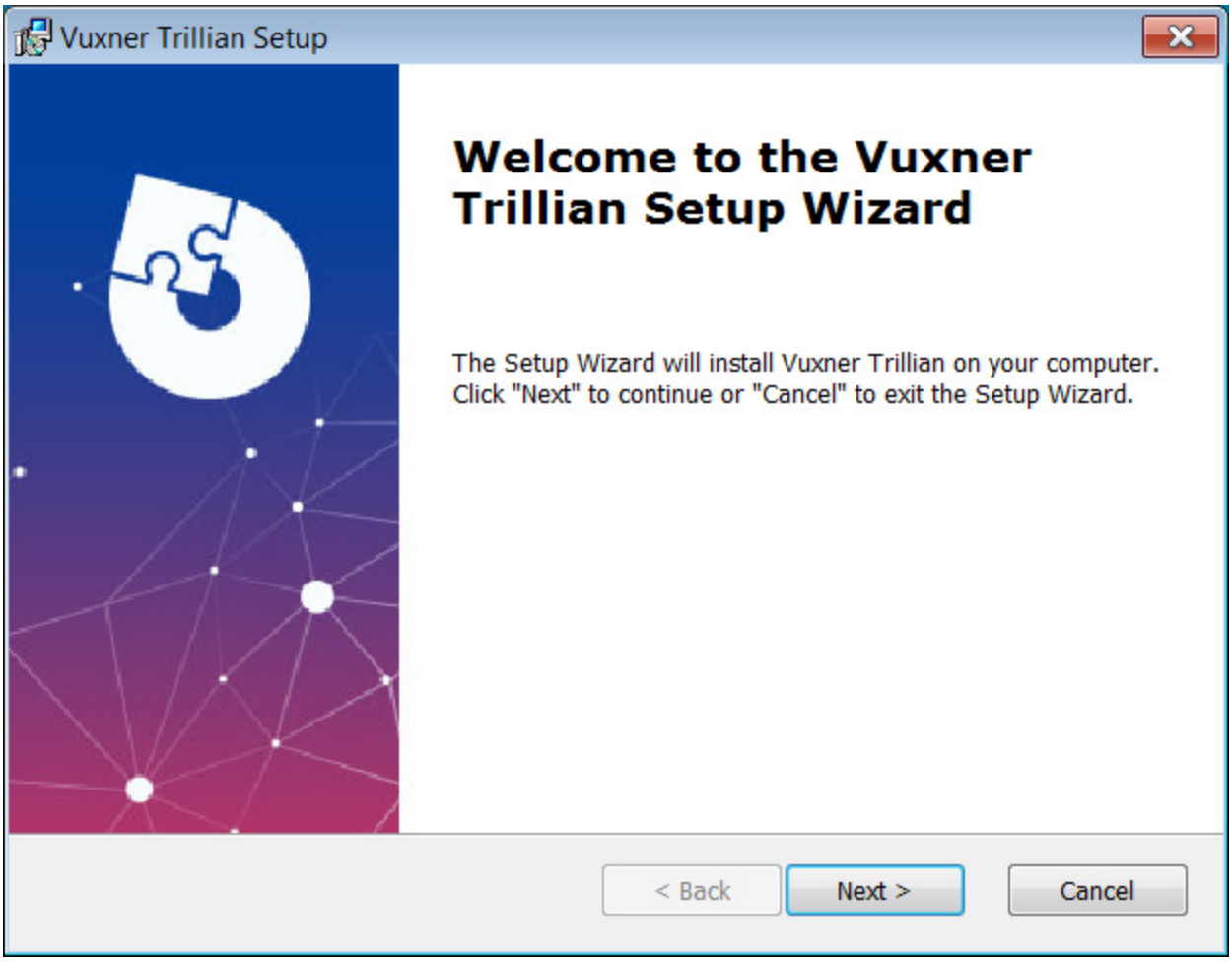
Google showed only a few results for 'Vuxner,' with one being for a well-designed and legitimate-looking vuxner[.]com, a site promoting "Vuxner Chat – Next level of privacy with free instant messaging."



Threat actor's Vuxner[.]com site to deploy malware

As this appeared to be the "Vuxner chat" the threat actors referenced in their email, BleepingComputer attempted to download it and run it on a virtual machine.

BleepingComputer found that the VuxnerChat.exe download [VirusTotal] actually installs the "Trillian" messaging app and then downloads further malware onto the computer after Trillian finishes installing.



Vuxner download installs Trillian

As this type of campaign looked similar to other campaigns that have pushed remote access and password-stealing trojans in the past, BleepingComputer reached out to cybersecurity firm Cluster25 who has previously helped BleepingComputer diagnose similar malware attacks in the past.

Fake Vuxner chat used to install a RAT

Cluster25 researchers explain in a report coordinated with BleepingComputer that the Vuxner[.]com is hosted behind Cloudflare, however they could still determine hosting server's actual address at 86.104.15[.]123.

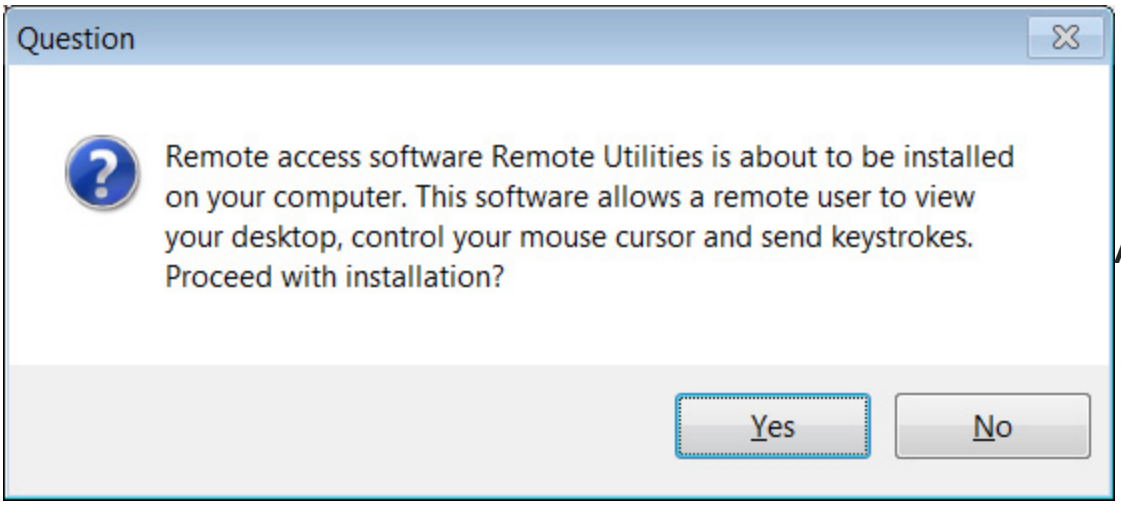
The researchers state that the Vuxner Chat program is being used as a decoy for installing a remote desktop software known as RuRAT, which is used as a remote access trojan.

"Infection chain for this campaign can be divide in a fist stage phase, where the decoy URL drops and installs a Software called “**Trillian**” and the second one where the installer drops a legitimate **Remote Desktop Software** known as **RuRAT** used for malicious purposes," the Cluster25 researchers explain.

Once a user installs the Vuxner Trillian client and exits the installer, it will download and execute a Setup.exe executable [VirusTotal] from https://vuxner[.]com/setup.exe

When done, the victim will be left with a C:\swrbldin folder filled with a variety of batch files, VBS scripts, and other files used to install RuRAT on the device.

Strangely, both Cluster25 and BleepingComputer saw the RAT installation ask us to confirm the installation of the software. This prompt is a sloppy giveaway that something nefarious is happening and should cause immediate suspicion when displayed.



Asking permission to install the RAT

Cluster25 told BleepingComputer that the threat actors are using this attack to gain initial access to a device and then take control over the host.

Once they control the host, they can search for credentials and sensitive data or use the device as a launchpad to spread laterally in a network.

As you can see, threat actors are willing to create elaborate campaigns consisting of fake sites, custom installers, and targeted emails to infect their victims.

For this reason, all business owners and consumers need to be wary of any unusual emails stating that you need to download something to communicate with them.

Receiving emails like the one BleepingComputer received should automatically be seen as suspicious, and recipients should research to determine if a particular software is legitimate or not.

Simply searching and seeing a single result related to a particular program is a huge red flag indicating that the program should be avoided.

At this time, BleepingComputer is not aware of any other companies or media outlets targeted by this malicious campaign, indicating that this is a limited spear-phishing campaign.

Related Articles:

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

Hackers target Russian govt with fake Windows updates pushing RATs

Ukraine supporters in Germany targeted with PowerShell RAT malware

Google exposes tactics of a Conti ransomware access broker

- Investor
- Malware
- RAT
- Remote Access Trojan
- Spear Phishing
- VC
- Venture Capitalist

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: