

Fake “Corona Antivirus” distributes BlackNET remote administration tool

blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/

Threat Intelligence Team

March 23, 2020



Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company’s network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

Corona Antivirus – World's best | X

antivirus-covid19.site

Corona Antivirus

Get started in 30 seconds

Download our Corona Antivirus application to start the protection.

01

The best COVID-19 Antivirus – directly from the research team

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app.

Privacy & Cookies Policy

Show all X

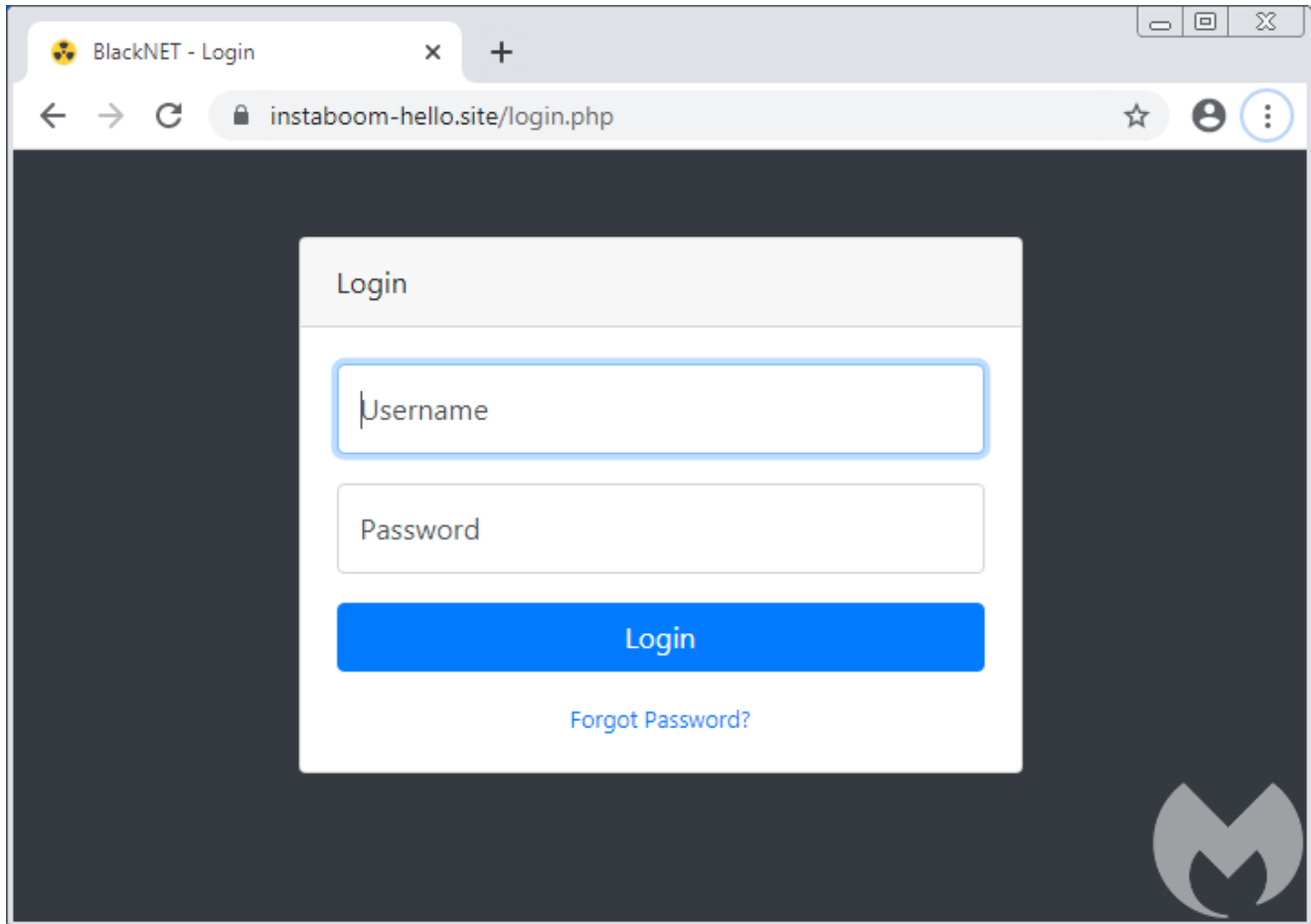
update.exe

Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed]
hxxps[://]instaboom-hello[.]site//getCommand[.]php?[removed]
hxxps[://]instaboom-hello[.]site//receive[.]php?command=[removed]
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was published on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security. x

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#). x

Slaves Menu

0 Total Clients!

0 USB Clients!

0 Online Clients!

0 Offline Clients!

Bot/Slaves List

Show entries Search:


<input type="checkbox"/>	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command	Execute
<input type="text" value="Select Command"/>	<input type="button" value="Send Command"/>

Map Visualization



Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



Malware blocked by Real-Time Protection

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: [MachineLearning/Anomalous.96%](#)

Path: C:\update.exe

[View Quarantine](#)[Close](#)

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

antivirus-covid19[.]site

Bogus corona antivirus

antivirus-covid19[.]site/update.exe

146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4

C2 panel

instaboom-hello[.]site