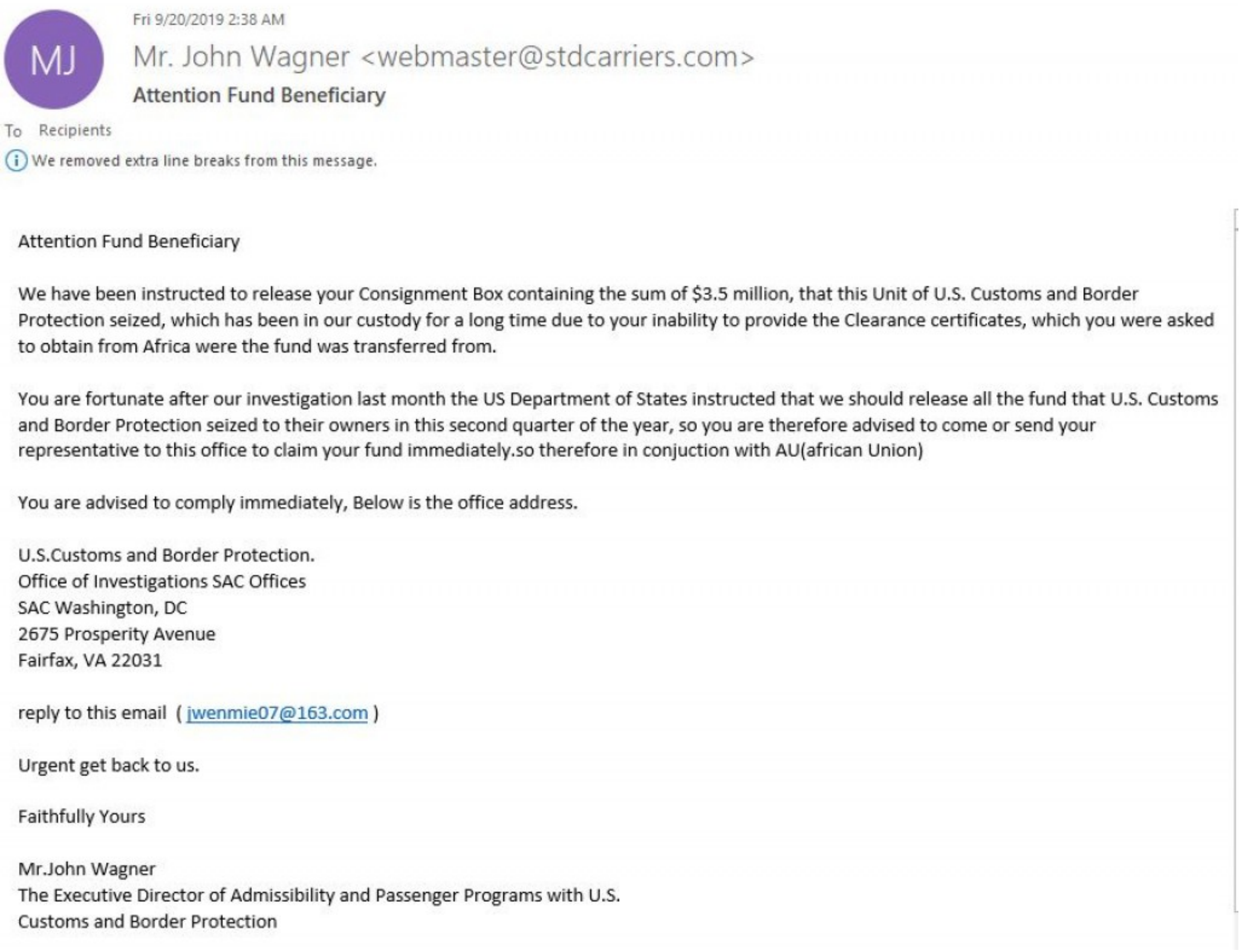
STD Registry Mail Server Hijacked by Spammers

Spammers were able to exploit a vulnerability in hMailServer and get the website's IP address blacklisted because the owner did not check the right box



MJ

Fri 9/20/2019 2:38 AM

Mr. John Wagner <webmaster@stdcarriers.com>

Attention Fund Beneficiary

To Recipients

We removed extra line breaks from this message.

Attention Fund Beneficiary

We have been instructed to release your Consignment Box containing the sum of $3.5 million, that this Unit of U.S. Customs and Border Protection seized, which has been in our custody for a long time due to your inability to provide the Clearance certificates, which you were asked to obtain from Africa were the fund was transferred from.

You are fortunate after our investigation last month the US Department of States instructed that we should release all the fund that U.S. Customs and Border Protection seized to their owners in this second quarter of the year, so you are therefore advised to come or send your representative to this office to claim your fund immediately.so therefore in conjuction with AU(african Union)

You are advised to comply immediately, Below is the office address.

U.S.Customs and Border Protection.
Office of Investigations SAC Offices
SAC Washington, DC
2675 Prosperity Avenue
Fairfax, VA 22031

reply to this email (jwenmie07@163.com)

Urgent get back to us.

Faithfully Yours

Mr.John Wagner
The Executive Director of Admissibility and Passenger Programs with U.S.
Customs and Border Protection

Portland, Sep 30, 2019 (Issuewire.com) - The revival of STD Carriers Disease Control and Prevention Services was crippled this past week when spammers hijacked its mail server by exploiting a vulnerability in hMailServer. As a result, the domain is now blacklisted by popular email providers and cannot contact its users. This also means that many authors of STD reports cannot recover their passwords and people seeking removal cannot contact the authors. Everything would have been prevented had the right box been checked in hMailServer.

STDCarriers.com was a nationally recognized sexually transmitted disease (STD) prevention service in 2012 before going offline. As part of reviving the site, an email was sent to registered users hoping to draw traffic back. Shortly after that a bot began exploiting a vulnerability in hMailServer and made the STD Carriers server send tens of thousands of bulk emails pitching a famous scam. STD Carriers suspects these emails to be connected to the ChaosCC Hacking Group which has been spamming STD Carriers with ransom demands in recent weeks. The suspicious timing indicates that at least one STD

Carriers account belongs to ChaosCC and ChaosCC attacked STD Carriers for the purpose of getting them blacklisted so that they could not communicate with thousands of users that have no idea the site is back.

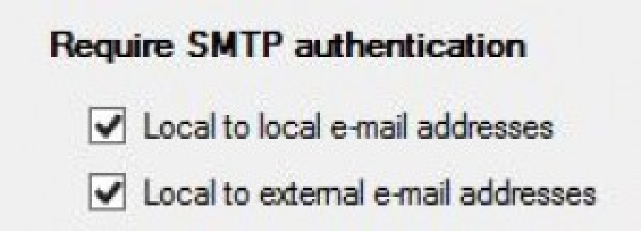
hMailServer has been one of the most popular open-source email server programs since 2002. It is a favourite of novices that are running their own mail server for the first time. The owner of STD Carriers is one of those people. He did not check the box to require authentication for internal to external messages. This is an easy mistake that anyone could make and hMailServer could do more to warn people about the importance of that box. The lesson to be learned here is that if you use hMailServer check that box.

For more information visit:

STD Carriers Disease Control and Prevention Services
https://stdcarriers.com

Fixing the Problem on the hMailServer Forum
https://www.hmailserver.com/forum/viewtopic.php?f=7&t=34387&p=214954

STDCarriers.com is Back Following Long Legal Battle
https://stdcarriers.com/news/articles/149-stdcarriers+com+is+back+following+long+legal+battle.aspx



Require SMTP authentication

☑ Local to local e-mail addresses

☑ Local to external e-mail addresses

Media Contact

CopBlaster.com

webmaster@copblaster.com

5039089256

P.O. Box 86653

Source : STDCarriers.com

See on IssueWire : https://www.issuewire.com/std-registry-mail-server-hijacked-by-spammers-1646135169497767