[PL #40486] FW: [2YCN08QS645] plannet-lab used for e-mail spoofing and password phishing

Michael J Freedman via RT support at planet-lab.org
Wed Nov 12 23:36:04 EST 2008

- Previous message: [PL #40484] Permission denied (publickey,keyboard-interactive)
- Next message: [PL #40489] Planetlab LUMS node Issue
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Email Recipients (see http://www.planet-lab.org/Support)
       Owner: Nobody
       Requestor: pike at netlab.uky.edu
       Ticket Ccs: jsli at ebay.com

================================================

Hi,

This issue came up also this summer with ebay, and we properly resolved
it (see email below).  I was hoping that .nyud.net addresses might have
been added to a whitelist, but this is the second time this has happened
since.  My previous experience was that some of eBay's security alerts
had some concurrency issues, such that I was simultaneously receiving
follow-on warnings/complaints from their department while receiving
personalized "resolved" emails such as the one below.

Anyway, I can assure that that CoralCDN is not involved in a phishing
scam.  More information about this academic research project can be
found at:

   http://www.coralcdn.org/

In short, it operates as a semi-open free webcache/CDN that you simple
need to modify a URL to access (ebay.com becomes ebay.com.nyud.net).
But we don't modify content in any way, and it takes special effort to
avoid the security problems of many open proxies (no cookies, no
CONNECT, no POST, no SSL, x-forwarded-for headers, special URL
modifications needed, etc.).

I'm cc'ing Justin Li in the hopes that CoralCDN might be added to ebay's
whitelist:  From before, it appeared that ebay has a direct line to
Google's (and hence FireFox's) domain blacklisting, so we'd like to
avoid this in the future.

Justin:  please let me know if I could be of more assistance.  It might
help to reference the previous ebay ticket # 2VMWB08GN329 from this July
for resolution.

Thanks,
Mike Freedman
CoralCDN Project


-------- Original Message --------
Subject: RE: [eBay:2VMWB08GN329] eBay.com e-mail spoofing and password
phishing
Date: Sat, 26 Jul 2008 11:29:25 -0600
From: Johnson, Ryan <grjohnson at ebay.com>
To: Michael J Freedman <mfreed at CS.Princeton.EDU>,
CC: <securityalerts at ebay.com

Hello Michael,

I apologize for the lengthy response time. I have received your
messages, and carefully reviewed the site in question. At first glance,
the site appears to come up as a Phishing site, or Compromised URL, but
```

is as you described, a site which is using the proxy on its own address.
It appears that one of our agents entered this site in by error, and
notices are still being sent because your reply had not been fully
investigated for some reason. I can assure you that We have taken
correct action regarding the issue, and have removed this site from our
database as being a suspect Phishing/Fraudulent site. We apologize for
any inconveniences that may have been caused, and assure you that we
would greatly appreciate your ability to resolve this from your end as
well and work more efficiently in the future if ever such a problem
arises.

Thank you,

Ryan Johnson
eBay Inc.
Audit and Investigations
grjohnson at ebay.com
securityalerts at ebay.com

\
Lowell Pike via RT wrote:
> *Email Recipients (see http://www.planet-lab.org/Support)*
> *Requestor: pike at netlab.uky.edu*
>
>
> *==========*
>
> *Wed Nov 12 09:49:59 2008: Request 40486 was acted upon.*
> *Transaction: Ticket created by pike at netlab.uky.edu*
>
> *Subject: FW: [2YCN08QS645] plannet-lab used for e-mail spoofing and password phishing*
>
>
> *We have been notified by our campus IT security that*
> *ebay has sent the following about planet-lab being*
> *used for e-mail phishing.*
>
> *Could you please tell us what has/is happening and*
> *how you have corrected this issue.*
>
> *kind regards,*
> *Lowell Pike*
> *Laboratory for Advanced Networking*
> *University of Kentucky*
> *pike at netlab.uky.edu*
> *(859) 257-3391*
>
>
>
>
>> *From: Justin Li <jsli at ebay.com>*
>> *To: "herman at pop.uky.edu" <herman at pop.uky.edu>, "Lee, Robert S"*
>> *<robert at spin.net.uky.edu>*
>> *Date: Sat, 8 Nov 2008 01:45:44 -0500*
>> *Subject: [eBay:2YCN08QS645] eBay.com e-mail spoofing and password phishing*
>>
>>
>> *Dear University of Kentucky,*
>>
>>
>>
>> *We have just learned that your service is being used to display*
>> *false or "spoofed" eBay.com pages, apparently in an effort to steal*
>> *personal and financial information from consumers, and defraud eBay*
>> *users. Specifically, it appears that an University of Kentucky user*
>> *is sending unsolicited messages which misrepresent the sender as*
>> *eBay, and making false statements that encourage the recipient to go*
>> *to a page hosted by you at*
>>
>>
>>

>> 128.163.142.20 -
>> http://cgi.ebay.com.nyud.net:8090/ws/eBayISAPI.dll?ViewItem&rd=1&item=330278849
> 932&ssPageName=STRK:MEWA:IT&ih=014
>>
>>
>> asking to enter personal and account information. The purloined
>> information is then sent to an email account and, based on our
>> investigation of similar schemes, used to steal accounts and commit
>> other fraudulent acts including international credit card and wire
>> fraud.
>>
>>
>>
>> This matter is urgent - we believe that consumers have been falsely
>> directed to this page and may be fooled into divulging personal
>> information to a criminal if the page is not immediately disabled.
>> We ask that you immediately disable the site at
>> http://cgi.ebay.com.nyud.net:8090/ws/eBayISAPI.dll?ViewItem&rd=1&item=330278849
> 932&ssPageName=STRK:MEWA:IT&ih=014
>> as well as any associated email addresses, so that this fraudulent
>> scheme can be stopped. We further request that you provide us with
>> all contact information that you have for this user so that we may
>> provide this information to the proper law enforcement authorities.
>>
>>
>>
>> While we believe that the above information gives your company more
>> than a sufficient basis for disabling the page immediately, out of
>> caution we note that your user's unauthorized reproduction of eBay's
>> trademark and copyrighted materials violates federal law, and places
>> an independent legal obligation on your company to remove the
>> offending page(s) immediately upon receiving notice from eBay, the
>> owner of the copyrighted materials. Accordingly, the information
>> below serves as eBay's notice of infringement pursuant to the
>> Digital Millennium Copyright Act, 17 U.S.C. Section 512 (c)(3)(A):
>>
>>
>>
>> I, the undersigned, CERTIFY UNDER PENALTY OF PERJURY that I am the
>> agent authorized to act on behalf of the owner of certain
>> intellectual property rights, said owner being named eBay Inc. I
>> have a good faith belief that the website located at URL
>> http://cgi.ebay.com.nyud.net:8090/ws/eBayISAPI.dll?ViewItem&rd=1&item=330278849
> 932&ssPageName=STRK:MEWA:IT&ih=014
>> as its copyright in each page of its website and associated source
>> code. Please act expeditiously to remove or disable access to the
>> material or items claimed to be infringing.
>>
>>
>>
>> We sincerely appreciate your immediate attention to this important
>> matter. We would also appreciate if you would take steps to confirm
>> the accuracy of any contact information that your user may have
>> provided to you in establishing the account. Should you have any
>> accurate information that could assist eBay and law enforcement in
>> tracking this individual, we greatly appreciate your assistance, as
>> we know that you do not condone the use of your services for such
>> criminal purposes.
>>
>>
>>
>> Finally, please be advised that we have referred this issue to the
>> Federal Bureau of Investigation for their investigation. The F.B.I.
>> has requested that we convey to you in this message their request
>> that you preserve for 90 days all records relating to this web site,
>> including all associated accounts, computer logs, files, IP
>> addresses, telephone numbers, subscriber and user records,
>> communications, and all programs and files on storage media in
>> regard to all Internet connection information, pursuant to 18 U.S.C.
>> Section 2703(f). While we do not act as an agent of the FBI in
>> conveying this request, we do intend to fully cooperate with their

>> investigation, and encourage you to do so as well.
>>
>>
>>
>> Thank you,
>>
>>
>>
>> eBay Inc.
>>
>> Audit and Investigations
>>
>> securityalerts at ebay.com
>>
>>
>>
>> Get automated, real-time notifications of new phishing attacks!
>> Join the Phish Report Network as a RECEIVER today!
>> http://www.phishreport.net/
>
>
>
> ------ End of Forwarded Message
>
> _____
> PlanetLab Support Mail Reflector
> support at planet-lab.org
> https://lists.planet-lab.org/mailman/listinfo/support-community

---

- Previous message: [PL #40484] Permission denied (publickey,keyboard-interactive)
- Next message: [PL #40489] Planetlab LUMS node Issue
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the support-community mailing list