Gerhard W Recher

04.12.2006 09:16

To: "BLKA [redacted] (Postfach)" <[redacted]>
cc:
Subject: Re: WG: [netpilot] Spammer with account at your site please close hi m !

Hallo Frau [redacted].

wie kann man in Zukunft die Sache beschleunigen ?
immer an diese Mail-adr ? ' [redacted] oder ... wie ...

Gruß

Gerhard W. Recher
(Geschäftsführer)

NETpilot GmbH

Wilhelm-Riehl-Str. 13
D-80687 München

Tel: ++49 89 547182 0
Fax: ++49 89 547182 33
GSM: ++49 171 4802507

w3: http://www.netpilot.net
e-Mail: mailto:Gerhard.Recher@netpilot.net

==========

diese mail gin an den Server-betreiber:

Der sirs

please close immediatly this offendig server with a ebay Phishing site !!!!

```
href="http://61.91.29.162/old/index.html
">https://signin.ebay.com/ws/eBayISAPI.dll?SignIn</a>
```

yours

Gerhard W. Recher
(Geschäftsführer)

NETpilot GmbH

Wilhelm-Riehl-Str. 13
D-80687 München

Tel: ++49 89 547182 0
Fax: ++49 89 547182 33
GSM: ++49 171 4802507

w3: http://www.netpilot.net
e-Mail: mailto:Gerhard.Recher@netpilot.net

========== offending mail leading to this server

Received: from relayn.netpilot.net ([127.0.0.1])
 by localhost (newtunix [127.0.0.1]) (clean-mx, port 10024)
with ESMTP
 id 08207-01; Thu, 30 Nov 2006 23:04:59 +0100 (CET)
Received: from book.netpilot.net (book.netpilot.net
[62.67.241.12])
          by relayn.netpilot.net (Postfix) with ESMTP id
E3C8238C006;
          Thu, 30 Nov 2006 23:04:02 +0100 (CET)
Received: from User (h-66-134-39-107.mclnva23.covad.net
[66.134.39.107])
          by book.netpilot.net (Postfix on SuSE Linux 8.0
(i386)) with ESMTP id D22374DCC1;
          Thu, 30 Nov 2006 22:59:08 +0100 (CET)
From: "eBay Inc."<service@ebay.com>
Subject: Your eBay Inc. account information needs to be
updated !
Date: Thu, 30 Nov 2006 16:59:15 -0500
MIME-Version: 1.0
Content-Type: text/html;
          charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Message-Id: <20061130215908.D22374DCC1@book.netpilot.net>
To: undisclosed-recipients:;
X-Virus-Scanned: by netpilot GmbH at clean-mx.de

<IMG src="
http://pics.ebaystatic.com/aw/pics/navbar/redesign_p1/ebayLogo
.gif"
border=0></A>
<P><FONT size=2><FONT face=Verdana>Dear valued
<STRONG><STRONG><SPAN style="FONT-SIZE:
10pt; COLOR: black; FONT-FAMILY: Verdana">eBay
Inc.</SPAN></STRONG>
</STRONG>member</FONT>:
</FONT>
</P>
<P><FONT size=2><FONT face=Verdana>It has come to our
attention that your <SPAN
style="FONT-SIZE: 10pt; COLOR: black; FONT-FAMILY:
Verdana"><STRONG>eBay
  Inc.</STRONG></SPAN> account information needs to be
  updated as part of our continuing commitment to protect your
account and to
reduce
the instance of fraud on our website.</P>
<P><FONT face=Verdana size=2> If you could please take 5-10
minutes

  of your </FONT><FONT face=Verdana size=2>online </FONT><FONT
face=Verdana
size=2>experience
  and update your personal records you will not run into

```
  any future </FONT><FONT face=Verdana size=2>problems with
the online
service.</FONT></P>
<P><FONT face=Verdana size=2>However, failure to update your
records will result in
account suspension. <BR>Please update your records on or
before <FONT
color=red><STRONG>December 15, 2006</STRONG>.</FONT>
<BR><BR>Once you have updated your
account records, your <SPAN style="FONT-SIZE: 10pt; COLOR:
black; FONT-FAMILY:
Verdana"><STRONG>eBay Inc.</STRONG></SPAN> session will
continue as normal. </FONT></P>

<P><FONT face=Verdana size=2>To update your <SPAN
style="FONT-SIZE: 10pt; COLOR: black;
FONT-FAMILY: Verdana"><STRONG>eBay
  Inc.</STRONG></SPAN> records click on the following link:
<BR>
  </FONT><br>
  <FONT face=Verdana size=2><a
href="http://61.91.29.162/old/index.html
">https://signin.ebay.com/ws/eBayISAPI.dll?SignIn</a></FONT></
P>
<P>Thank You.  <BR>
  <SPAN style="FONT-SIZE: 10pt; COLOR: black; FONT-FAMILY:
Verdana"><STRONG>eBay
  Inc.</STRONG></SPAN></P>
<P><FONT face=Verdana size=2></FONT> </P>

<P><FONT face=Verdana size=2>Accounts Management As outlined
in our User Agreement, <SPAN
style="FONT-SIZE: 10pt COLOR: black FONT-FAMILY:
Verdana"><STRONG>eBay
Inc.</STRONG></SPAN> will <BR>periodically send you
information about site changes and
enhancements. </FONT></P>
<P><FONT face=Verdana size=2>Visit our Privacy Policy and User
Agreement if you
  have any questions. <BR>
  <a target="_parent"
href="
http://pages.ebay.com/help/policies/hub.html?ssPageName=f:f:US
">http://pages.ebay.com/help/policies/</A></FONT></P>
==========
```

----- Forwarded by Gerhard W Recher/Netpilot/DE on 30.11.2006 23:55 -----

Gerhard W Recher

30.11.2006 23:40

To: abuse@web.de, abuse@yahoo.com, abuse@google.de, abuse@covad.net, abuse@t-ipnet.de, abuse-isp@covad.com

cc: [redacted]

Subject: [netpilot] Spammer with account at your site please close him !

Dear sirs,

recently a spammer abused a weak customer account at our facilities.

1) this subject submitted 3 test-mails to own accounts at your mail-platform (google, yahoo.com and web.de) please close them / and /or identify him!! see following log-fragment

Nov 29 23:27:25 book postfix/smtpd[17617]: DFD1A4DD63:
client=p508B6A4F.dip.t-dialin.net[80.139.106.79], sasl_method=LOGIN, sasl_username=web4
Nov 29 23:27:26 book postfix/cleanup[17621]: DFD1A4DD63:
message-id=<20061129222725.DFD1A4DD63@book.netpilot.net>
Nov 29 23:27:26 book postfix/qmgr[22239]: DFD1A4DD63: from=<secure@ebay.com>, size=749,
nrcpt=3 (queue active)
Nov 29 23:27:28 book postfix/smtp[17622]: DFD1A4DD63: to=<danimad@gmail.com>,
relay=relayn.netpilot.net[62.67.240.20]:25, delay=3.1, delays=0.67/0.04/0.01/2.4, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as AB5C2EAC1F0)
Nov 29 23:27:28 book postfix/smtp[17622]: DFD1A4DD63: to=<d_a_n_i_m_a_d@web.de>,
relay=relayn.netpilot.net[62.67.240.20]:25, delay=3.1, delays=0.67/0.04/0.01/2.4, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as AB5C2EAC1F0)
Nov 29 23:27:28 book postfix/smtp[17622]: DFD1A4DD63: to=<d_a_n_i_m_a_d@yahoo.com>,
relay=relayn.netpilot.net[62.67.240.20]:25, delay=3.1, delays=0.67/0.04/0.01/2.4, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as AB5C2EAC1F0)
Nov 29 23:27:28 book postfix/qmgr[22239]: DFD1A4DD63: removed

2) he used a foreign machine (zombie ?) to further abuse this weak account at our customer site.

Nov 30 22:54:29 book postfix/smtpd[31758]: 7BC654DD13:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4
Nov 30 22:54:38 book postfix/smtpd[31758]: 19CA84DD14:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4
Nov 30 22:54:47 book postfix/smtpd[31758]: 58A9E4DD19:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4
Nov 30 22:54:57 book postfix/smtpd[31758]: 364624DD1A:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4

3) we closed this account.

yours

Gerhard W. Recher
(Geschäftsführer)

NETpilot GmbH

Wilhelm-Riehl-Str. 13
D-80687 München

Tel: ++49 89 547182 0
Fax: ++49 89 547182 33
GSM: ++49 171 4802507

w3: http://www.netpilot.net
e-Mail: mailto:Gerhard.Recher@netpilot.net

==========

inetnum: 80.128.0.0 - 80.146.159.255
netname: DTAG-DIAL16
descr: Deutsche Telekom AG
country: DE
admin-c: DTIP
tech-c: DTST
status: ASSIGNED PA
remarks: **********
remarks: * Abuse Contact: http://www.t-com.de/ip-abuse in case of Spam, *
remarks: * Hack Attacks, Illegal Activity, Violation, Scans, Probes, etc. *
remarks: **********
mnt-by: DTAG-NIC
source: RIPE # Filtered

person: DTAG Global IP-Addressing
address: Deutsche Telekom AG
address: D-90492 Nuernberg
address: Germany
phone: +49 180 5334332
fax-no: +49 180 5334252
e-mail: ripe.dtip@telekom.de
nic-hdl: DTIP
mnt-by: DTAG-NIC
source: RIPE # Filtered

person: Security Team
address: Deutsche Telekom AG
address: Germany
phone: +49 180 5334332
fax-no: +49 180 5334252
e-mail: abuse@t-ipnet.de
nic-hdl: DTST
mnt-by: DTAG-NIC
source: RIPE # Filtered

NetRange: 66.134.0.0 - 66.134.255.255
CIDR: 66.134.0.0/16
NetName: COVAD-IP-2-NET
NetHandle: NET-66-134-0-0-1
Parent: NET-66-0-0-0-0
NetType: Direct Allocation
NameServer: NS3.COVAD.COM

NameServer: NS4.COVAD.COM
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
Comment:
Comment: for abuse issues, please contact abuse-isp@covad.com
Comment: Reassignment information for this block of addresses can be found at rwhois://rwhois.laserlink.net:4321/
RegDate: 2001-07-13
Updated: 2004-03-11

RAbuseHandle: CART-ARIN
RAbuseName: Covad abuse reporting team
RAbusePhone: +1-703-376-2830
RAbuseEmail: abuse-isp@covad.com

RTechHandle: ZC178-ARIN
RTechName: Admin
RTechPhone: +1-888-801-6285
RTechEmail: ip_admin@covad.com

OrgAbuseHandle: CART-ARIN
OrgAbuseName: Covad abuse reporting team
OrgAbusePhone: +1-703-376-2830
OrgAbuseEmail: abuse-isp@covad.com

"BLKA [redacted] (Postfach)" <[redacted]>

[redacted]25
[redacted]@polizei.b
[redacted]

04.12.2006 08:58

To: "'gerhard.recher@netpilot.net'" <gerhard.recher@netpilot.net>
cc:
Subject: WG: [netpilot] Spammer with account at your site please close him!

Hallo Herr Recher,

könnten Sie mit bitte noch die gesamte u.g. Phishing-Mail mit Quelldaten schicken.
Ich werde die Daten dann an die zuständige Dienststelle zur weiteren Bearbeitung weiterleiten.

Mit freundlichen Grüßen

N[redacted]
Bayerisches Landeskriminalamt
SG 625 – Wirtschaftsdelikte
Maillingerstraße 15, 80636 München
mailto:[redacted]
☎ [redacted]

-----Ursprüngliche Nachricht-----
Von: [redacted]
Gesendet: Freitag, 1. Dezember 2006 12:02
An: [redacted]
Betreff: WG: [netpilot] Spammer with account at your site please close him !

-----Ursprüngliche Nachricht-----
Von: Gerhard W. Recher [mailto:gerhard.recher@netpilot.net]
Gesendet: Freitag, 1. Dezember 2006 11:53
An: [redacted]
Betreff: [netpilot] Spammer with account at your site please close him !

Hallo Herr [redacted],

Hier hat sich offensichtlich deutscher Internetteilnehem am versand von Phising Mails geübt....
Sollen wir Ihn anzeigen ? was benötigen Sie von uns ?

Er kam von:

Nov 29 23:27:25 book postfix/smtpd[17617]: DFD1A4DD63:
client=p508B6A4F.dip.t-dialin.net[80.139.106.79], sasl_method=LOGIN, sasl_username=web4

das ist irgentwo in essen...

Gruß

Gerhard W. Recher
(Geschäftsführer)

NETpilot GmbH

Wilhelm-Riehl-Str. 13
D-80687 München

Tel: ++49 89 547182 0
Fax: ++49 89 547182 33
GSM: ++49 171 4802507

w3: http://www.netpilot.net
e-Mail: mailto:Gerhard.Recher@netpilot.net

----- Forwarded by Gerhard W Recher/Netpilot/DE on 01.12.2006 11:58 -----

Gerhard W Recher
30.11.2006 23:40

To: abuse@web.de, abuse@yahoo.com, abuse@google.de, abuse@covad.net, abuse@t-ipnet.de, abuse-isp@covad.com
cc: [redacted]
Subject: [netpilot] Spammer with account at your site please close him !

Dear sirs,

recently a spammer abused a weak customer account at our facilities.

1) this subject submitted 3 test-mails to own accounts at your mail-platform (google, yahoo.com and web.de) please close them / and /or identify him!! see following log-fragment

Nov 29 23:27:25 book postfix/smtpd[17617]: DFD1A4DD63:
client=p508B6A4F.dip.t-dialin.net[80.139.106.79], sasl_method=LOGIN, sasl_username=web4
Nov 29 23:27:26 book postfix/cleanup[17621]: DFD1A4DD63:
message-id=<20061129222725.DFD1A4DD63@book.netpilot.net>
Nov 29 23:27:26 book postfix/qmgr[22239]: DFD1A4DD63: from=<secure@ebay.com>, size=749,
nrcpt=3 (queue active)
Nov 29 23:27:28 book postfix/smtp[17622]: DFD1A4DD63: to=<danimad@gmail.com>,
relay=relayn.netpilot.net[62.67.240.20]:25, delay=3.1, delays=0.67/0.04/0.01/2.4, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as AB5C2EAC1F0)
Nov 29 23:27:28 book postfix/smtp[17622]: DFD1A4DD63: to=<d_a_n_i_m_a_d@web.de>,
relay=relayn.netpilot.net[62.67.240.20]:25, delay=3.1, delays=0.67/0.04/0.01/2.4, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as AB5C2EAC1F0)
Nov 29 23:27:28 book postfix/smtp[17622]: DFD1A4DD63: to=<d_a_n_i_m_a_d@yahoo.com>,
relay=relayn.netpilot.net[62.67.240.20]:25, delay=3.1, delays=0.67/0.04/0.01/2.4, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as AB5C2EAC1F0)
Nov 29 23:27:28 book postfix/qmgr[22239]: DFD1A4DD63: removed

2) he used a foreign machine (zombie ?) to further abuse this weak account at our customer site.

Nov 30 22:54:29 book postfix/smtpd[31758]: 7BC654DD13:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4
Nov 30 22:54:38 book postfix/smtpd[31758]: 19CA84DD14:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4
Nov 30 22:54:47 book postfix/smtpd[31758]: 58A9E4DD19:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4
Nov 30 22:54:57 book postfix/smtpd[31758]: 364624DD1A:
client=h-66-134-39-107.mclnva23.covad.net[66.134.39.107], sasl_method=LOGIN,
sasl_username=web4

3) we closed this account.

yours

Gerhard W. Recher
(Geschäftsführer)

NETpilot GmbH

Wilhelm-Riehl-Str. 13
D-80687 München

Tel: ++49 89 547182 0
Fax: ++49 89 547182 33
GSM: ++49 171 4802507

w3: http://www.netpilot.net
e-Mail: mailto:Gerhard.Recher@netpilot.net

==========

inetnum: 80.128.0.0 - 80.146.159.255
netname: DTAG-DIAL16
descr: Deutsche Telekom AG
country: DE
admin-c: DTIP
tech-c: DTST
status: ASSIGNED PA
remarks: **********
remarks: * Abuse Contact: http://www.t-com.de/ip-abuse in case of Spam, *
remarks: * Hack Attacks, Illegal Activity, Violation, Scans, Probes, etc. *
remarks: **********
mnt-by: DTAG-NIC
source: RIPE # Filtered

person: DTAG Global IP-Addressing
address: Deutsche Telekom AG
address: D-90492 Nuernberg
address: Germany
phone: +49 180 5334332
fax-no: +49 180 5334252
e-mail: ripe.dtip@telekom.de
nic-hdl: DTIP
mnt-by: DTAG-NIC
source: RIPE # Filtered

person: Security Team
address: Deutsche Telekom AG
address: Germany
phone: +49 180 5334332
fax-no: +49 180 5334252
e-mail: abuse@t-ipnet.de
nic-hdl: DTST
mnt-by: DTAG-NIC
source: RIPE # Filtered

NetRange: 66.134.0.0 - 66.134.255.255
CIDR: 66.134.0.0/16
NetName: COVAD-IP-2-NET
NetHandle: NET-66-134-0-0-1
Parent: NET-66-0-0-0-0
NetType: Direct Allocation
NameServer: NS3.COVAD.COM
NameServer: NS4.COVAD.COM
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
Comment:
Comment: for abuse issues, please contact abuse-isp@covad.com
Comment: Reassignment information for this block of addresses can be found at rwhois://rwhois.laserlink.net:4321/
RegDate: 2001-07-13
Updated: 2004-03-11

RAbuseHandle: CART-ARIN
RAbuseName: Covad abuse reporting team
RAbusePhone: +1-703-376-2830
RAbuseEmail: abuse-isp@covad.com

RTechHandle: ZC178-ARIN
RTechName: Admin
RTechPhone: +1-888-801-6285
RTechEmail: ip_admin@covad.com

OrgAbuseHandle: CART-ARIN
OrgAbuseName: Covad abuse reporting team
OrgAbusePhone: +1-703-376-2830
OrgAbuseEmail: abuse-isp@covad.com