Gerhard W Recher

01.12.2006 11:53

To: L[redacted] Ka[redacted] <[redacted]>
cc:
Subject: [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

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