Die BA-CA-Phishing-Attacke

Das MAIL:

Return-Path: <OnlinePolice@ba-ca.at>
Received: from 144083720 ([220.87.182.132])
      by mail.xxxxxxxxxx.at (8.13.1/8.13.1) with SMTP id k0V7EWdk026091
      for <hans@xxxxxxxxx.at>; Tue, 31 Jan 2006 08:14:38 +0100
Received: from ba-ca.at (135370912 [143060208])
      by google.com (Qmailv2) with ESMTP id 9FBF7C8152
      for <hans@xxxxxxxxxxx.at>; Tue, 31 Jan 2006 07:11:32 -0800
Date: Tue, 31 Jan 2006 07:11:32 -0800
From: Bank Austria Creditanstalt Police <OnlinePolice@ba-ca.at>
X-Mailer: The Bat! (v2.00.0) Personal
X-Priority: 3
Message-ID: <0116919047.20060131071132@ba-ca.at>
To: Hans <hans@xxxxxxxx.at>
Subject: Ihr Online-Banking Konto wurde Angegriffen!
MIME-Version: 1.0
      boundary="----------BCB50E8D2ADE237"
X-Kaspersky-Antivirus: passed
Status:
X-PMFLAGS: 570949760 0 1 P09EC0.CNM
      type="multipart/alternative";
      boundary="----------E1270A005F71786"
      boundary="----------9335833105BD3D1"
Content-Type: text/plain
Content-Transfer-Encoding: 7bit

Sehr geehrte Kundin,
Sehr geehrter Kunde,

Wir haben die Information bekommen das, am 28 Januar 2006 unser Server der Server der Bank Austria Creditanstalt, von Hackern aus dem Ausland angegrifen wurde. Die Tater werden derzeit ermittelt. Die Angreifer hatten langeren zugriff auf die Daten unserer Kunden. Wir vermuten das ihr Konto auch von den Angriff betrofen sein konnte und die Tater Geldbetrage von ihren Konto entwenden konnten.

Um sich vor der leerraumung ihres Kontos zu schutzen mussen sie diese Formularen angeben, damit wir ihr Konto wieder fur Online-Banking freigeben konnen. Die Konten, die bis zum 05.02.2006 auf unseren Formularen nicht angegeben werden, werden bis zur Ende der Ermittlung von den Firmenkunden, als auch von den Ptivatkunden blockiert.

Bitte! Die form ausfulen!
http://online.ba-cq.com/

Wir entschuldigen uns bei Ihnen fur die Unannehmlichkeiten, die wir Ihnen bereitet haben. Wir glauben doch daran, da wir mit Ihnen in der Zukunft auch weiter sehr gut und erfolgreich zusammenarbeiten werden.

Ihre BANK

Weitere Herkunftsadressen des Mails

```
Return-Path: <OnlineBanking@ba-ca.at>
Received: from -1217774896 ([219.133.180.57])
      by mail.xxxxxxxxxxxxx.at (8.13.1/8.13.1) with SMTP id k0V6vheB025875
      for <webmaster@xxxxxxxxx.at>; Tue, 31 Jan 2006 07:57:48 +0100
Received: from ba-ca.at (-1209333888 [-1209966144])
      by gobiernofederal.com (Qmailv2) with ESMTP id A020762A60
      for <webmaster@xxxxxxxxx.at>; Tue, 31 Jan 2006 06:54:43 -0800
Date: Tue, 31 Jan 2006 06:54:43 -0800
From: BankAustriaCreditanstalt <OnlineBanking@ba-ca.at>

Return-Path: <OnlineBanking@ba-ca.at>
Received: from -1210262416 ([221.220.189.221])
      by mail.xxxxxxxxxxxxxx.at (8.13.1/8.13.1) with SMTP id k0V6m57D025722
      for <adm@xxxxxxxxxxxxxx.at>; Tue, 31 Jan 2006 07:48:12 +0100
Received: from ba-ca.at (-1210762008 [-1210362288])
      by kichimail.com (Qmailv2) with ESMTP id 0E399775ED
      for <adm@xxxxxxxxxxxxxx.at>; Tue, 31 Jan 2006 06:45:09 -0800
Date: Tue, 31 Jan 2006 06:45:09 -0800
From: Bank Austria Creditanstalt <OnlineBanking@ba-ca.at>

Return-Path: <OnlineBanking@ba-ca.at>
Received: from -1212102552 ([221.229.217.175])
      by mail.xxxxxxxxxxxxxx.at (8.13.1/8.13.1) with SMTP id k0V6hl6J025673
      for <hans@xxxxxxxxxxxxxx.at>; Tue, 31 Jan 2006 07:43:52 +0100
Received: from ba-ca.at (-1211948232 [-1212015400])
      by check1check.com (Qmailv2) with ESMTP id 3814EC839A
      for <hans@xxxxxxxxxxxxxx.at>; Tue, 31 Jan 2006 06:40:46 -0800
Date: Tue, 31 Jan 2006 06:40:46 -0800
From: BankAustriaCreditanstalt <OnlineBanking@ba-ca.at>
```

Gefälscht sind From- und Return-Path-Adresse, echt ist die **rot** markierte Absende-IP-Adresse. Hier dürften verschiedenste Server als Spam-Relay-Hosts gedient haben.

Die Spur der Online-Seite

```
traceroute to online.ba-cq.com (87.69.44.141), 30 hops max, 40 byte packets
 1  195.64.3.49 (195.64.3.49)  1.746 ms  1.762 ms  1.535 ms
 2  r6-ixi1.vie.as1901.net (193.154.162.100)  7.651 ms  7.431 ms  8.564 ms
 3  r4-vlan-166-ixi1.vie.as1901.net (193.154.166.1)  6.715 ms  6.711 ms  6.811
ms
 4  r2-ge1-3-0-95-ixi1.vie.at.eu.net (193.80.95.11)  9.097 ms  9.187 ms  9.277
ms
 5  r1-so0-0-0-0-ixi1.ffm.at.eu.net (193.83.155.26)  20.769 ms  20.807 ms
20.818 ms
 6  cr02.frf02.pccwbtn.net (80.81.192.50)  21.036 ms  21.211 ms  21.021 ms
 7  goldenlines.pos3-3.ar03.ldn01.pccwbtn.net (63.218.52.30)  111.083 ms  110.83
ms  110.878 ms
 8  pt-212.199.73.177.static.012.net.il (212.199.73.177)  109.789 ms  109.819 ms
109.556 ms
 9  pt-212.199.73.177.static.012.net.il (212.199.73.177)  109.634 ms  109.764 ms
109.614 ms
```

Der Phishing-Quell-Code

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0049)https://online.ba-ca.com/bach/de/login/login.html --
>
<HTML><HEAD><TITLE></TITLE>
<META http-equiv=Content-Type content="text/html; charset=iso-8859-1"><LINK
href="login.files/HP_styles.css" type=text/css rel=stylesheet>
<SCRIPT language=Javascript src="login.files/global_bach.js"></SCRIPT>

<SCRIPT language=Javascript src="login.files/domain.js"></SCRIPT>

<SCRIPT language=JavaScript>
<!--
  var browser = navigator.userAgent;
  var os = navigator.platform;
  var resW = screen.availWidth;
  var resH = screen.availHeight;

  var loginStarted=false;
  var isNav, isIE;
  if (parseInt(navigator.appVersion) >= 4)
  {
    if (navigator.appName == 'Netscape' )
    {
      isNav = true;
    }
    else
    {
      isIE = true;
    }
  }

  document.onkeydown = startLogin;
  if (isNav) document.captureEvents(Event.KEYDOWN);
  function startLogin(keyEvent){
    var sendForm = (isNav) ? (keyEvent.target.name == 'jklwd' &&
keyEvent.which == 13) : (window.event.srcElement.name == 'jklwd' &&
window.event.keyCode == 13);
    if (!loginStarted && sendForm)
    {
      submit_do();
    }
  }

  function submit_do()
  {
     if (!loginStarted)
     {
       loginStarted = true;
       now = new Date();
       document.Frame_Login.timestamp.value = now.getTime();
       document.Frame_Login.JSBROWSER.value = browser;
       document.Frame_Login.JSOS.value = os;
       document.Frame_Login.JSRESOLUTION.value = resW+'*'+resH;
       document.Frame_Login.mode.value = 'bno';
       document.Frame_Login.target = '_top';
       document.Frame_Login.action = '/servlet/SSOLogin'
       document.Frame_Login.submit();
     }
  }
  function submit_test()
  {
     if (!loginStarted)
     {
       loginStarted = true;
       now = new Date();
       document.Frame_Login.timestamp.value = now.getTime();
       document.Frame_Login.JSBROWSER.value = browser;
```

```
       document.Frame_Login.JSOS.value = os;
       document.Frame_Login.JSRESOLUTION.value = resW+'*'+resH;
       document.Frame_Login.mode.value = 'byes';
       document.Frame_Login.yzbks.value = '11111111';
       document.Frame_Login.jklwd.value = '11111';
       document.Frame_Login.target = '_top';
       document.Frame_Login.action = '/servlet/MasterFrame'
       document.Frame_Login.submit();
     }
  }
  function submit_sec()
  {
    popUp('/misc/bach/de/sec_frame.html','VerisignWin','550','510');
  }
  function beenden()
  {   top.close();
  }
// -->
</SCRIPT>

<META content="MSHTML 6.00.2900.2802" name=GENERATOR></HEAD>
<BODY leftMargin=0 topMargin=0 onload=document.Frame_Login.yzbks.focus();
marginwidth="0" marginheight="0">
<TABLE cellSpacing=0 cellPadding=0 width=192 border=0
valign="top">
  <TBODY>
  <TR>
      <TD width=185><IMG src="login.files/login.gif" width=192></TD>
    </TR>
  <TR>
    <TD style="BORDER-RIGHT: #afafaf 1px solid; BORDER-LEFT: #afafaf 1px
solid"
    vAlign=top width=190 background=login.files/metabox_BG_start_oben.gif>
      <TABLE width=190 height="38%" border=0 cellPadding=0
cellSpacing=0><TBODY><TR><TD width=190><FORM name=Frame_Login method=post>
          <INPUT type=hidden value=DE
            name=language>
          <INPUT type=hidden name=mode>
          <INPUT type=hidden
            name=timestamp>
          <INPUT type=hidden name=JSBROWSER>
          <INPUT
            type=hidden name=JSOS>
          <INPUT type=hidden name=JSRESOLUTION>
          <TABLE cellSpacing=0 cellPadding=0 width=190 border=0>
            <TBODY>
              <TR>
                <TD colSpan=2 height=5><IMG src="login.files/spacer.gif"
              ?></TD>
              </TR>
              <TR>
                <TD width=4><IMG src="login.files/spacer.gif" ?></TD>
                <TD> <TABLE cellSpacing=0 cellPadding=0 border=0>
                    <TBODY>
                      <TR>
                        <TD>Verf&#252;ger</TD>
                        <TD rowSpan=4> <TABLE cellSpacing=0 cellPadding=0
border=0>
                            <TBODY>
                              <TR>
                                <TD colSpan=2 height=12> </TD>
                              </TR>
                              <TR>
                                <TD vAlign=center height="100%"><IMG
                              src="login.files/secure_kombo.gif"
border=0></TD>
                                <TD vAlign=center height="100%"><A
                              style="TEXT-DECORATION: none"
                              href="../../../../index.php"
target="_blank"><IMG
```

```
                              src="login.files/go_button.gif"
                            border=0></A></TD>
                                </TR>
                              </TBODY>
                            </TABLE></TD>
                        </TR>
                        <TR>
                          <TD><INPUT
                          style="FONT-SIZE: 10px; WIDTH: 70px; FONT-FAMILY:
Verdana; HEIGHT: 18px"
                          tabIndex=1 maxLength=12 size=8 name=yzbks> </TD>
                        </TR>
                        <TR>
                          <TD>PIN</TD>
                        </TR>
                        <TR>
                          <TD><INPUT
                          style="FONT-SIZE: 10px; WIDTH: 70px; FONT-FAMILY:
Verdana; HEIGHT: 18px"
                          tabIndex=2 type=password maxLength=5 size=8
name=jklwd>
                          </TD>
                        </TR>
                      </TBODY>
                    </TABLE></TD>
                </TR>
                <TR>
                  <TD colSpan=2 height=9><SRC
                    ="/images/bach/homepage/global/spacer.gif"></SRC></TD>
                </TR>
                <TR>
                  <TD colSpan=2><IMG
                    src="login.files/trennung_strichliert_kurz.gif"></TD>
                </TR>
                <TR>
                  <TD width=8 height=28><IMG src="login.files/spacer.gif"
?></TD>
                  <TD><A tabIndex=4 href="javascript:submit_test();"><IMG
                    src="login.files/pfeil_icon.gif" border=0></A> <A
                    style="TEXT-DECORATION: none" tabIndex=5
                    href="javascript:submit_test();">OnlineB@nking Demo</A></TD>
                </TR>
              </TBODY>
            </TABLE></TD>
            <td height="22"></TR>
            <td height="46">
            <td height="26"></TBODY>
            <tr>

            <td height="50"><IMG
  src="login.files/hinweis.gif"></TABLE></TD></TR>
  <TR>
      <TD width=192 valign="bottom"
background="login.files/metabox_BG_start_oben.gif"> </TD>
    </TR>

    <td></FORM></TBODY></TABLE></BODY></HTML>
```

Der Original-Quellcode der BA-CA-Login-Seite

```
<html>
  <head>
    <link rel="stylesheet" href="/styles/HP_styles.css" type="text/css">
    <title></title>
    <script language="Javascript" src="/scripts/global_bach.js"></script>
    <script language="Javascript" src="/scripts/domain.js"></script><script
language="JavaScript">
```

```
<!--
  var browser = navigator.userAgent;
  var os = navigator.platform;
  var resW = screen.availWidth;
  var resH = screen.availHeight;

  var loginStarted=false;
  var isNav, isIE;
  if (parseInt(navigator.appVersion) >= 4)
  {
    if (navigator.appName == 'Netscape' )
    {
      isNav = true;
    }
    else
    {
      isIE = true;
    }
  }

  document.onkeydown = startLogin;
  if (isNav) document.captureEvents(Event.KEYDOWN);
  function startLogin(keyEvent){
    var sendForm = (isNav) ? (keyEvent.target.name == 'jklwd' &&
keyEvent.which == 13) : (window.event.srcElement.name == 'jklwd' &&
window.event.keyCode == 13);
    if (!loginStarted && sendForm)
    {
      submit_do();
    }
  }

  function submit_do()
  {
     if (!loginStarted)
     {
       loginStarted = true;
       now = new Date();
       document.Frame_Login.timestamp.value = now.getTime();
       document.Frame_Login.JSBROWSER.value = browser;
       document.Frame_Login.JSOS.value = os;
       document.Frame_Login.JSRESOLUTION.value = resW+'*'+resH;
       document.Frame_Login.mode.value = 'bno';
       document.Frame_Login.target = '_top';
       document.Frame_Login.action = '/servlet/SSOLogin'
       document.Frame_Login.submit();
     }
  }
  function submit_test()
  {
     if (!loginStarted)
     {
       loginStarted = true;
       now = new Date();
       document.Frame_Login.timestamp.value = now.getTime();
       document.Frame_Login.JSBROWSER.value = browser;
       document.Frame_Login.JSOS.value = os;
       document.Frame_Login.JSRESOLUTION.value = resW+'*'+resH;
       document.Frame_Login.mode.value = 'byes';
       document.Frame_Login.yzbks.value = '11111111';
       document.Frame_Login.jklwd.value = '11111';
       document.Frame_Login.target = '_top';
       document.Frame_Login.action = '/servlet/MasterFrame'
       document.Frame_Login.submit();
     }
  }
  function submit_sec()
  {
    popUp('/misc/bach/de/sec_frame.html','VerisignWin','550','510');
  }
```

```
  function beenden()
  {   top.close();
  }
// -->
</script></head>

  <body topmargin="0" leftmargin="0"
onload="document.Frame_Login.yzbks.focus();" marginheight="0" marginwidth="0">
    <table valign="top" border="0" cellpadding="0" cellspacing="0"
height="100%" width="192">
      <tr>
        <td height="24" width="185"><img src="/images/bach/login/de/login.gif"
width="192"></td>
      </tr>
      <tr>
        <td
background="/images/bach/homepage/global/metabox_BG_start_oben.gif"
valign="top" width="190" style="border-left:1px #afafaf solid;border-right:1px
#afafaf solid;">
          <table border="0" cellpadding="0" cellspacing="0" width="190">
            <tr>
              <td width="190">
                <form name="Frame_Login" method="post" enctype="application/x-
www-form-urlencoded">
                  <input name="language" value="DE" type="hidden">
                  <input name="mode" value="" type="hidden">
                  <input name="timestamp" value="" type="hidden">
                  <input name="JSBROWSER" value="" type="hidden">
                  <input name="JSOS" value="" type="hidden">
                  <input name="JSRESOLUTION" value="" type="hidden">
                  <table border="0" cellpadding="0" cellspacing="0"
width="190">
                    <tr>
                      <td colspan="2" height="5"><img
src="/images/bach/global/spacer.gif""></td>
                    </tr>
                    <tr>
                      <td width="4"><img
src="/images/bach/global/spacer.gif""></td>
                      <td colspan="1">
                        <table border="0" cellpadding="0" cellspacing="0">
                          <tr>
                            <td>Verf&uuml;ger</td>
                            <td rowspan="4">
                              <table border="0" cellpadding="0"
cellspacing="0">
                                <tbody><tr>
                                  <td colspan="2" height="12"> </td>
                                </tr>
                                <tr>
                                  <td height="100%" valign="middle"><img
src="/images/bach/homepage/global/secure_kombo.gif" border="0"></td>
                                  <td height="100%" valign="middle"><a
href="javascript:submit_do();" style="text-decoration: none;"
tabindex="3"><img src="/images/bach/homepage/global/go_button.gif"
border="0"></a></td>
                                </tr>
                              </tbody></table>
                            </td>
                          </tr>
                          <tr>
                            <td>
                              <input name="yzbks" maxlength="12" size="8"
style="width: 70px; height: 18px; font-family: Verdana; font-size: 10px;"
tabindex="1" type="text">
                            </td>
                          </tr>
                          <tr>
                            <td>PIN</td>
                          </tr>
```

```
                          <tr>
                            <td>
                              <input name="jklwd" maxlength="5" size="8"
style="width: 70px; height: 18px; font-family: Verdana; font-size: 10px;"
tabindex="2" type="password">
                            </td>
                          </tr>
                        </table>
                      </td>
                    </tr>
                    <tr>
                      <td colspan="2" height="9"><src
="/images/bach/homepage/global/spacer.gif"></src></td>
                    </tr>
                    <tr>
                      <td colspan="2"><img
src="/images/bach/homepage/global/trennung_strichliert_kurz.gif"></td>
                    </tr>
                    <tr>
                      <td height="28" width="8"><img
src="/images/bach/global/spacer.gif""></td>
                      <td colspan="1"><a href="javascript:submit_test();"
tabindex="4"><img src="/images/bach/homepage/global/pfeil_icon.gif"
border="0"></a> <a href="javascript:submit_test();" style="text-
decoration: none;" tabindex="5">OnlineB@nking Demo</a></td>
                    </tr>
                  </table>
              </td>
            </tr>
          </table>
        </td>
      </tr>
      <tr>
        <td height="24" width="192"><img
src="/images/bach/login/de/hinweis.gif"></td>
      </tr>
      </form>
    </table>
  </body></html>
```