Faked Libraries

COLLABORATORS			
	TITLE : Faked Libraries		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		July 10, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

Faked Libraries

1.1 List of registered names of libraries

```
                -- WARNING ---- WARNING ---- WARNING ---- WARNING ---- WARNING  ↩
                   ---- WARNING --


   This is a list of faked libraries: V2 - 11.02.99


                rexxkuang11.library

                datatypes.library
                -- WARNING ---- WARNING ---- WARNING ---- WARNING ---- WARNING  ↩
                   ---- WARNING --
```

1.2 Fake of rexxkuang11.library

```
$VER: Kuang11Update.readme 2.35 (06.02.99) Kuang11 Update changes

05.02.98

*********************************************************
**********                                     **********
**********  Virus warning! You MUST read this!  **********
**********                                     **********
*********************************************************



VIRUS VIRUS VIRUS VIRUS VIRUS VIRUS VIRUS VIRUS VIRUS VIRUS


XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Warning
****

All Kuang Eleven users who have received an update in the past few weeks are at risk!

Two viruses have been released via the update server attached to different versions of the file rexxkuang11.library (normally placed in LIBS:), and also affecting the file C:Mount.

Details
****

The two versions of the library which were infected are shown below, along with some details:

rexxkuang11.library 0.36 (4/02/99)
==========
- File size: 31,172
- Attaches itself to your C:Mount file (any version) unless SnoopDOS is running
- Performs "run >NIL: newshell TCP:2551" (both the library and C:Mount)
- Allows remote CLI (shell) access to your computer
- Calls itself "Vaginitis #2" by "STD"
- Does NOT spread to any other files (other than C:Mount)

rexxkuang11.library 0.27 (27/12/98)
==========
- File size: 26,532 bytes
- Performs "RUN >NIL: newshell tcp:2333" when the library is opened
- Allows remote CLI (shell) access to your computer
- Calls itself "Vaginitis #3" by "STD"
- Does NOT spread to any other files

Solution
****

· You should have received version 0.37 (or later) of rexxkuang11.library with this update. You should verify this by typing:

Version LIBS:rexxkuang11.library FILE FULL

You should get the response:

rexxkuang11.library 0.37 (5/02/99)

or a later version.

· Reboot your system (if possible, do NOT go online).

· Replace the file C:Mount from your original disks, or some other reliable source.

· Reboot AGAIN.

If you have any copies of rexxkuang11.library versions 0.27 and 0.36,
they should be deleted, as these were never legitimately uploaded to the
update server.

Explanation
****

The server at which the Amiga Coding Syndicate's updates are stored was
hacked by an unknown, malicious person or persons. We have changed our
passwords and have made every effort to secure our site.

We sincerely regret any inconvenience this has caused anyone.

If you wish to eliminate auto-updates from your Kuang Eleven installation,
simply rename or delete the file Rexx/Kuang11UPD.amirx (relative to your
AmIRC directory).

****

1.3 Fakes of datatype.library

-- WARNING ---- WARNING ---- WARNING ---- WARNING ---- WARNING ---- WARNING --

Info from Virus Checker VT3.13 (11.01.99):
   Please don't use the following datatypes.library at your system.

  datatypes.library   Size: 32832   Version: 45.5   Date: (17.02.98)
  datatypes.library   Size: 32748   Version: 45.5   Date: (??.??.98)
  datatypes.library   Size: 30844   Version: 45.5   Date: (??.??.98)

   These are faked versions of the original system library.

Please install instead:

  datatypes.library   Size: 27780   Version: 45.4   Date: (28.06.97)
      Copyright: Roland 'Gizzy' Mainz - (GISBURN@w-specht.rhein-ruhr.de)
      Available: Aminet - util/libs/dtypes454upd.lha

      ****
      *   This is a posting from Stéphane Payet to all Amigians.   *
      ****

   From: Stéphane Payet <stephane.payet@wanadoo.fr>
   Date: 06.12.1998, 09:07:59
Subject: If you have datatypes.library v45.4 or 45.4 it is a pirat's trap ! (fwd)

```
Hi,

*** FORWARDED MESSAGE ***
  Original author: Stéphane Payet
  Written on: 06-Déc-98
*** Beginning of forwarded message ***

Hi,

This a small part of the annonce of Nordic Global:
-----------------------------------------------------------------
Official statement from Nordic Global Inc.           12/05/98
-----------------------------------------------

(originally written on 12/04/98, updated on 12/05/98)
Recommendations
---------------

As a user you should take the following precautions:

- Most passwords were exported through a Trojan in fake versions
  of "datatypes.library" (in "LIBS:"), distributed by a cracker
  group. The fake version has a file size of 32748 bytes, and
  "version" returns either 45.4 or 45.5, depending on how and
  when you check the version.

  If you have that version of the library installed then delete it,
  and replace it with a legitimite version. Either use one of the
  original Workbench versions (39.11 or 40.6), or get the "real"
  version 45.4 (file size: 27780 bytes) from Aminet, and install
  it instead.

  Versions that appear to be safe are: 39.11, 40.6, 45.3, and
  45.4 (but 45.4 only if it has a file size of 27780 bytes).

  After installing a safe version, switch your computer off, wait
  for 30 seconds, and switch it back on.

- Then IMMEDIATELY change the password on your ISP account. Don't
  waste time and effort trying to find out if you are on the list.
  This is pointless, because even if you are not on the list you
  don't know if your account information has become known to
  crackers after the list was compiled.

- There is NO need to change anything in the setup of your
  protocol stack (whether it is Miami, AmiTCP or anything else),
  or to switch protocol stacks, even if friends, dealers or other
  software companies recommend you to do that. In some cases
  known to me companies have, for whatever reasons, unfortunately
  given such incorrect advice to users. The attack was not related
  to or caused by a specific protocol stack.

Holger Kruse, Nordic Global Inc.
kruse@nordicglobal.com
-----------------------------------------------------------------
```

For more info go to the site and read news.

Regards.

Stéphane

*** End of forwarded message ***

Regards.

------END------