Unknown

From: Conus Joël
Sent: Tuesday, January 08, 2002 6:31 PM
To: Bongard Dominique; Brique Olivier; Christophe Nicolas; Gaillard Christophe; Groux Cédric; Guggenheim Alan; JJ Gee (E-mail); Kudelski Henri; Sasselli Marco
Subject: [ES]

Attachments: ES 20020108.txt.asc

ES 20020108.txt
(13 KB)

```
*** PGP SIGNATURE VERIFICATION ***
*** Status:   Good Signature
*** Signer:   Joël Conus <conus@Nagra.com> (0xACC187D8)
*** Signed:   1/8/2002 6:28:49 PM
*** Verified: 6/6/2007 12:16:39 AM
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***

Summary:
- The hackers have found an EMM to reopen the locked DNASP003 cards. They have been
using the brute force method to find candidate EMMs to achieve this task for over a week
now. A DNASP003 card can be unlocked by putting it in an AVR3 loaded with specific code.
According to the first reports, the success rate would be between 50% and 75%. We
already have a patch to counter this attack. [Ref. 1]
- The hackers are using the IDA Pro software to disassemble the IRD firmware. [Ref. 2]
- A new freeware PC-based emulator, Winvu 2.0.0.5, has been released. There is not
enough feedback yet to tell if it is working. Since it requires a special serial PCI
card installed in the PC, it is very unlikely that it will ever get a large user base.
DishEMU and Firepck2 which also need such a card are not very popular either. [Ref. 3]
- dsshead.com are selling an unlooper at USD 6999. This is probably a scam like all the
unloopers we've seen for sale on the Internet before. [Ref. 4]
- The owner of the site dssonline.org has been busted. [Ref. 5]
- The DNS e3mdish.com has been bought but the site is still empty. [Ref. 6]

-------------------------------------------------------------------------
Status
======

Original cards
--------------
DNASP002          : Hole open. Some cards have blocker software.
DNASP003          : Hole can be reopened. Some cards have blocker
                    software.
DNASP010          : Not compromised.
DNASP011          : Not compromised.

Blockers
--------
AVR3 w/ EEPROM    : Freeware. Autoroll. Down (MCG AR 2.00).
AVR3              : Freeware. Non-autoroll. Working (MCG 3.07).
AVR3 Live Flash   : Freeware. Semi-autoroll. The keys are updated
                    from the Internet while the device is in the IRD.
                    Working (MCG 3.07).
AVRH / EasyRoll   : Freeware. Semi-autoroll. The card has to contain
                    the current transmission keys. Down.
Superroll/Guardian: Commercial. Autoroll. Working.
```

```
Emulators (cardless)
---------
AVR3 Cardless     : Freeware. Reported not working
                    perfectly (blackouts) (NAWapo).
Phantom           : Commercial. AVR-based. Working.
Winvu 2.0.0.5     : Freeware. Autoroll. PC-based. Uses a modified
                    AVR3 for interface. Probably working.
Firepck2          : Freeware. Supposedly autoroll. PC-based. Possibly
                    working.
DishEMU           : Commercial. PC-based. Possibly working.

Unloopers (glitchers)
---------
None available.

------------------------------------------------------------------------

Disclaimer: the contents of this mail are made of gossips from the
            Internet. Therefore they cannot be considered as a
            reliable source of information.


*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```