

HP Printer Display Hack

<http://irongeek.com/i.php?page=security/hphack>

번역 : nina@wowhacker.org

This is an old hack (1997) and does not accomplish much, but it is fun! [Silicosis](#) of LOpht (sili@lOpht.com) wrote the original exploit code for *nix [systems](#) and someone else ported it to NT/2000/XP based systems. Although it's been out there for a long time, it still works on every [HP printer/JetDirect](#) box I have seen. What the HP display hack allows you to do is set the text that displays on the little LCD panel of an HP printer. **It accomplishes this over**



the network by sending packets to a JetDirect box hooked to the [printer](#) (or built into it).

이것은 오래된 hack(1997)이고, 그렇게 많이 성공하지는 않는다. 하지만 재밌다! LOpht의 [Silicosis\(sili@lOpht.com\)](#)은 *nix 시스템에 대한 오리지널 익스플루잇 코드를 작성했고, 다른 누군가는 그것을 NT/2000/XP 기반 시스템으로 포팅했다. 그렇게 한 것이 꽤나 오래 됐음에도 불구하고, 아직도 내가 봤던 모든 HP printer/JetDirect 에서 동작을 한다. HP display hack으로 할수 있는 것은 HP 프린터의 작은 LCD 패널에 표시되는 text를 설정하는 것이다. **JetDirect box가 hook된(혹은 내부에 built in 된것)Printer로 패킷을 보냄으로서 네트워크를 통해서도 된다**

The first thing you need to do is find out the IP or [hostname](#) of the JetDirect box that services the printer. You can do this in one of at least three ways. The first way is by hitting the little test button on the JetDirect box that's connected to the printer. If the JetDirect card is built in you may have to go through the menus and choose "Print Configuration". Another way is to go into your "Printers and Faxes" settings, right click and bring up the properties of the printer in question, and look under the Ports tab for the hostname (npi*****). Once you have this information it's easy to run Silicosis ' little hack.

첫번째로 해야하는 것은 JetDirect box가 서비스하는 프린터의 IP나 hostname을 찾는 것이다. 이것을 할수 있는 것은 적어도 3가지방법중에 하나로 할수 있다. 첫번째는 프린터에 연결되어 있는 JetDirect box에 있는 작은 test 버튼을 hitting하는 것이다. JetDirect card가 당신에게 built in되어 있다면, 메뉴를 지나야만 할것이고, "Print Configuration"을 선택한다. 다른 방법은 "Printers와 Faxes" 설정에 가서, 오른쪽을

클리하고, 프린터 속성으로 가서, Port tab 아래쪽에 host 이름(npi*****)을 찾아라. 한번 이 정보를 얻으면, Silicosis 의 little hack 은 하기가 쉬워진다.

To run it from Windows just use the following syntax: hpnt Hostname Message

윈도우에서 실행하기 위해서 다음의 간단한 사항만을 하면된다. : hpnt Hostname Message

Windows Example:

```
C:\>hpnt npi769e71 "Irongeek"
HP Display hack -- sili@lOpht.com
Hostname: npi769e71
Message: Irongeek
Connecting....
Sent 54 bytes

C:\>hpnt 192.168.1.14 "Irongeek Also"
HP Display hack -- sili@lOpht.com
Hostname: 192.168.1.14
Message: Irongeek Also
Connecting....
Sent 59 bytes

C:\>
```

If you want to run it from Linux download the [source code](#) at the bottom of this page and compile it using [gcc](#). The syntax is the same as the Windows version. Below is an example of how to compile and run it:

만약에 LINUX 에서 실행을 하고 싶다면, 이 페이지의 아래쪽에 있는 SOURCE CODE 를 받아서 gcc 를 사용하여 컴파일한다. Syntax 는 윈도우와 동일하다. 아래에 있는 것은 어떻게 컴파일 하고 실행하는지에 대한 예제이다.

```
[root@balrog root]# gcc -o hphack hp.c
hp.c:28:12: warning: multi-line string literals
are deprecated
[root@balrog root]# ./hphack
192.168.1.14 "Irongeek"
HP Display hack -- sili@lOpht.com
Hostname: 192.168.1.14
Message: Irongeek
```

```
Connecting....  
Sent 54 bytes  
[root@balrog root]#
```

A few ideas for messages: "Hey Baby", "X was Here", "I see You", "Redrum", "Kill".
Enjoy. I'm working on my own GUI version with extra features, it's [web page](#) will be [here](#) when it's done.

메시지 관련 아이디어들로는 Hey Baby", "X was Here", "I see You", "Redrum", "Kill"이 있을수 있겠다.

Enjoy 하시고, 나는 기타 다른 기능들과 함께 GUI 버전에 대해서 일하고 있는데, 그것에 대한 웹페이지는 그것에 완료되고 나면 여기에 있을 것이다.

Downloads:

[Unix Source](#)

[Windows Source](#)

[Windows Binary](#)



[Printable version of this article](#)

Ten most recent posts on Irongeek.com:

- [XAMPP: an easy to install Apache daemon containing MySQL, PHP and Perl](#)
- [Louisville InfoSec Conference Write-up](#)
- [RFID Show and Tell with Kn1ghtl0rd and lowtek mystik](#)
- [PhreakNIC, Louisville InfoSec, and two cool pen-testing projects](#)
- [Thumbscrew: Software USB Write Blocker](#)
- [Thumb Sucking: Automatically copying data off of USB flash drives](#)
- [Using Metagoofil to extract metadata from public documents found via Google](#)
- [Creating An Auto Hack USB Drive Using Autorun and Batch Files. By Dosk3n](#)
- [What can you find out from an IP?](#)
- [How To Burn An ISO Image To A Bootable CD](#)