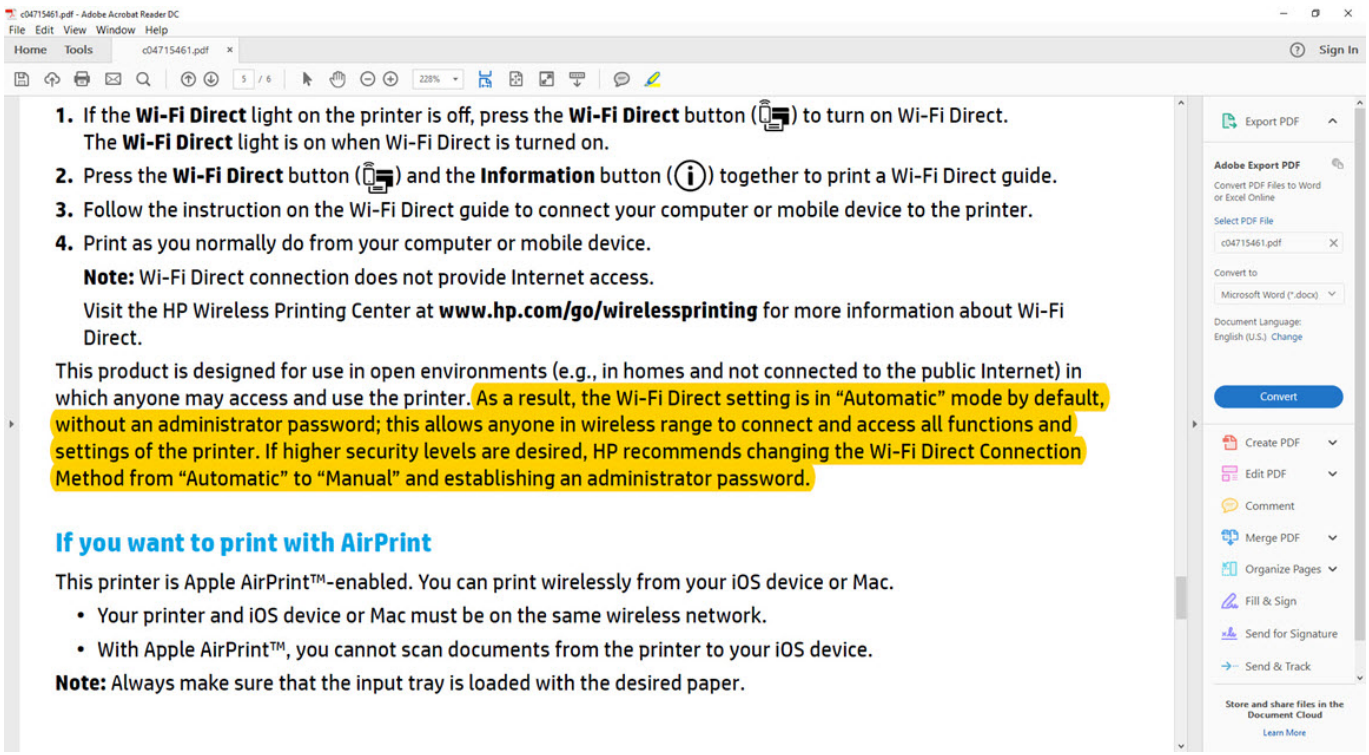
Don’t Underestimate Printers

written by Mert SARICA | 1 February 2018

A few months ago, upon my spouse’s need, I began searching for a printer. As someone who hadn’t owned a printer in their home for the past 15 years, I was pleased to find that the prices of printers on e-commerce websites had become much more reasonable in terms of both price and performance compared to years past. Adhering to the saying “Man is insatiable”, I wanted a cheap one, with a scanner, that could also make photocopies, had Wi-Fi support, and could easily print from mobile devices, and I came across HP’s DeskJet 3630 All-in-One printer and purchased it for 200 Turkish Liras.

Ignoring my spouse’s valid complaints of “don’t tinker with it, you’ll break it!”, I decided to quickly take a look at this new device that I would be including in my home’s local network. Using the HP Easy Start application, I

was able to quickly add the printer to my wireless network by entering the password for my existing Wi-Fi network in under five minutes and promptly completing the setup. In the setup steps, I did not see any guidance on matters that should be taken into consideration for security, such as setting a strong management interface password. However, this printer also had Wi-Fi Direct technology, which allows Wi-Fi devices to exchange data with each other. When I looked at the printer's setup documents, it was stated that for high security levels, the Wi-Fi setting should be changed from automatic to manual, but there was no information provided to the user on how to do this.



1. If the **Wi-Fi Direct** light on the printer is off, press the **Wi-Fi Direct** button ( ) to turn on Wi-Fi Direct. The **Wi-Fi Direct** light is on when Wi-Fi Direct is turned on.
2. Press the **Wi-Fi Direct** button ( ) and the **Information** button ( ) together to print a Wi-Fi Direct guide.
3. Follow the instruction on the Wi-Fi Direct guide to connect your computer or mobile device to the printer.
4. Print as you normally do from your computer or mobile device.

   Note: Wi-Fi Direct connection does not provide Internet access.

   Visit the HP Wireless Printing Center at **www.hp.com/go/wirelessprinting** for more information about Wi-Fi Direct.

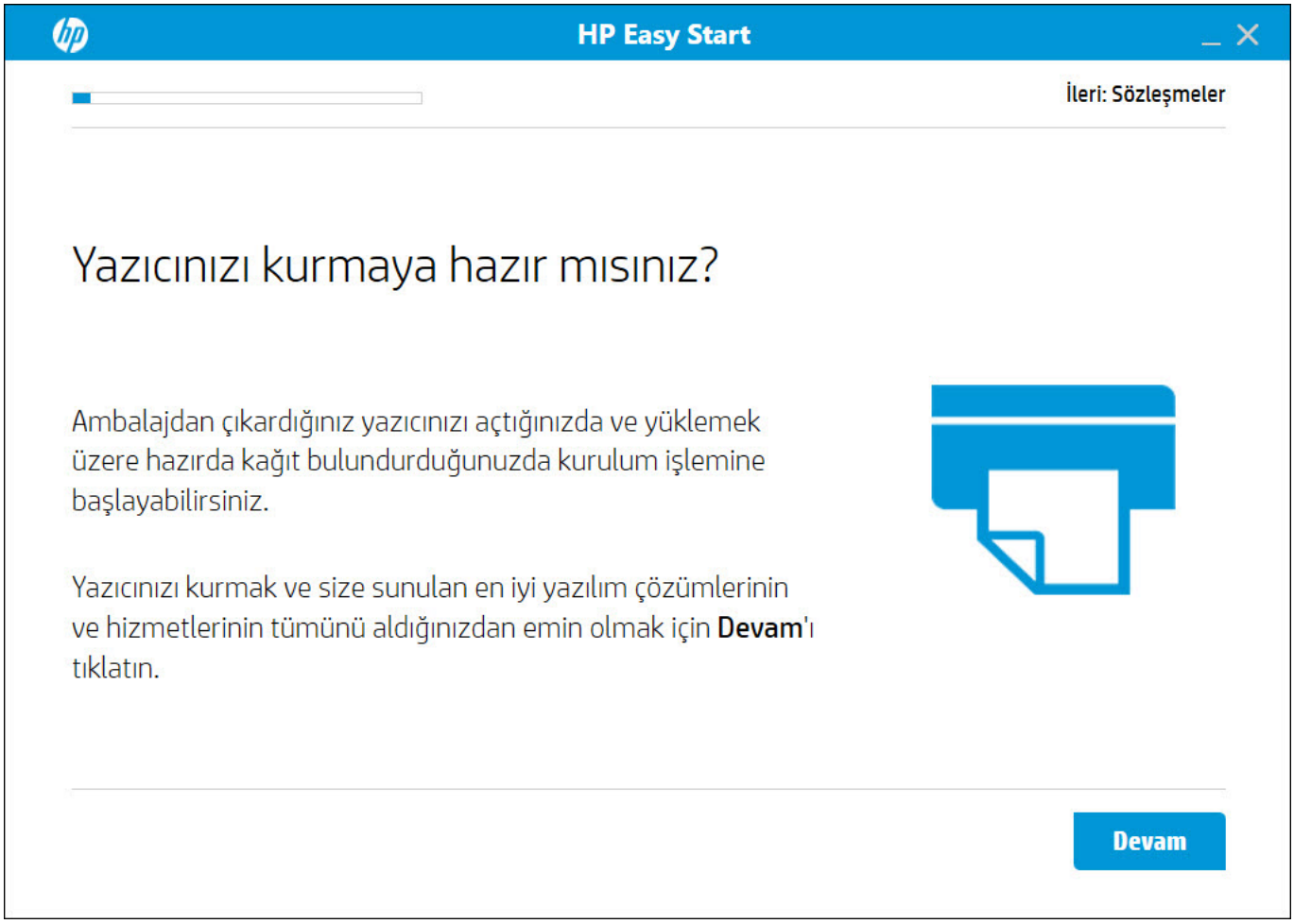
This product is designed for use in open environments (e.g., in homes and not connected to the public Internet) in which anyone may access and use the printer. As a result, the Wi-Fi Direct setting is in "Automatic" mode by default, without an administrator password; this allows anyone in wireless range to connect and access all functions and settings of the printer. If higher security levels are desired, HP recommends changing the Wi-Fi Direct Connection Method from "Automatic" to "Manual" and establishing an administrator password.

If you want to print with AirPrint

This printer is Apple AirPrint™-enabled. You can print wirelessly from your iOS device or Mac.

- Your printer and iOS device or Mac must be on the same wireless network.
- With Apple AirPrint™, you cannot scan documents from the printer to your iOS device.

Note: Always make sure that the input tray is loaded with the desired paper.



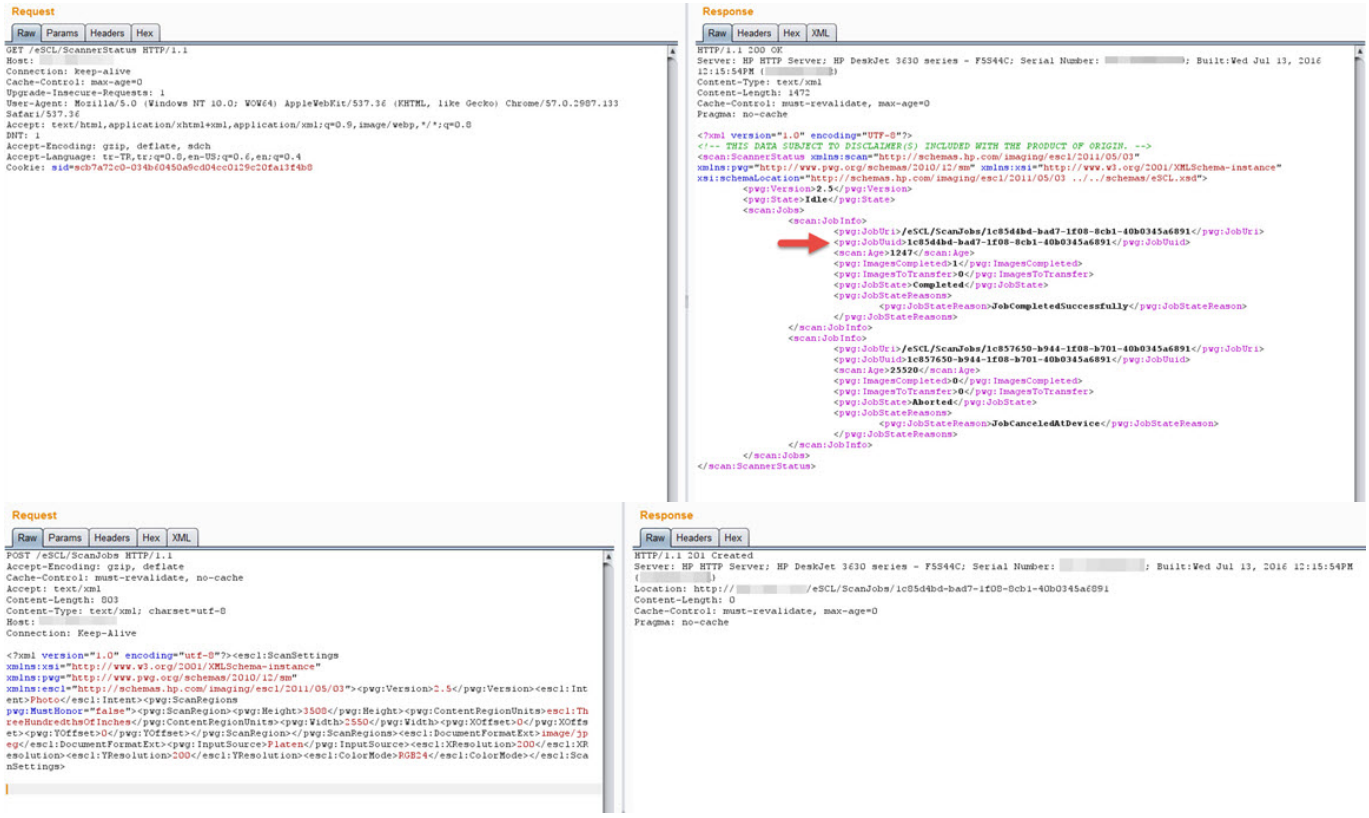
When I pressed the Wireless and Information buttons on the printer, I learned that the Wi-Fi Direct password was 12345678. The disappointing thing is that it should not have been so difficult for the user to change such a simple password during setup. As someone who prefers to tinker with a device rather than use it properly, I was left wondering “How could this default password for Wi-Fi Direct be misused?” and began searching for an answer.

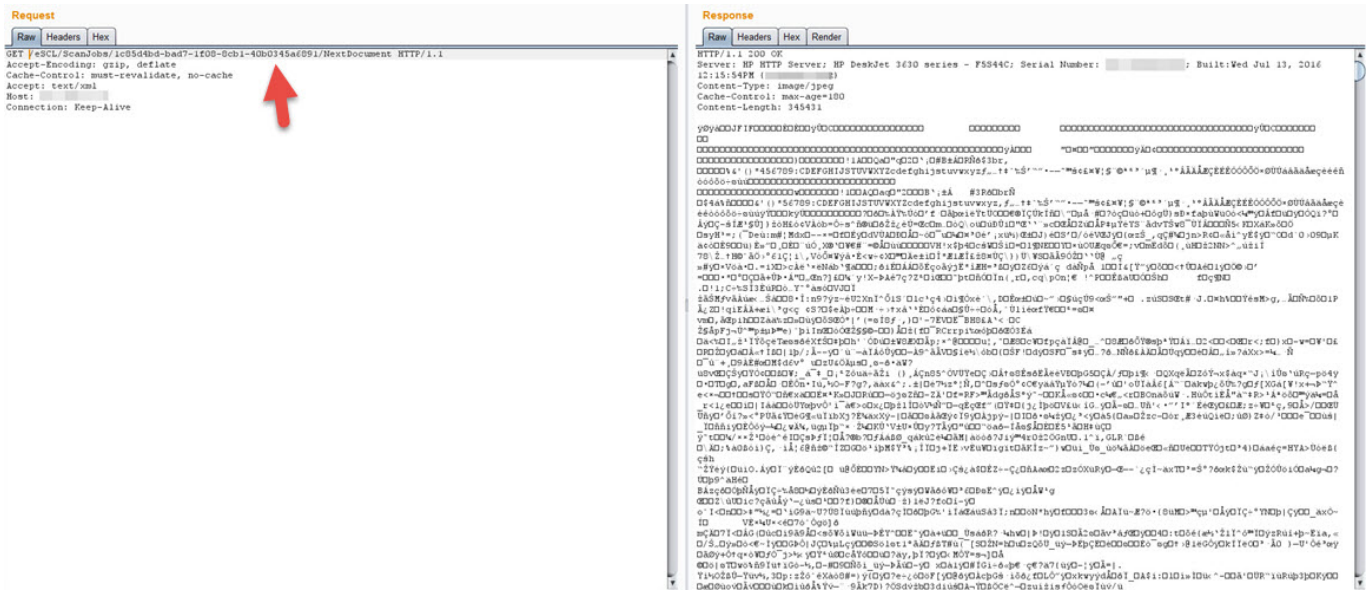
Imagine that in areas where there are many business centers and offices, from subscriber centers that occasionally process population papers, to notaries, this printer and scanner are actively used. Let one of the officials’ duties be to scan the population papers obtained from the customer during the process. Could a malicious person connect to the printer via Wi-Fi Direct with the password 12345678 and download an image file of a scanning process that has already been successfully completed from the printer? Fortunately, the answer to this question is no, because the printer does not allow the downloaded image file to be downloaded a second time, and probably also deletes it from memory.

But what if this malicious person were to monitor the status of the printer through a web service and, immediately after a scanning process starts and

ends, initiates and completes 1 more scanning process and downloads the image file? And what if he did this with a tool coded in Python and running on a Raspberry Pi? We can imagine how different the situation would be. Although I haven't done any work on the Raspberry Pi side, I decided to quickly develop a small tool called HP Scanner Thief in Python to demonstrate how easy it could be to misuse it and create awareness.

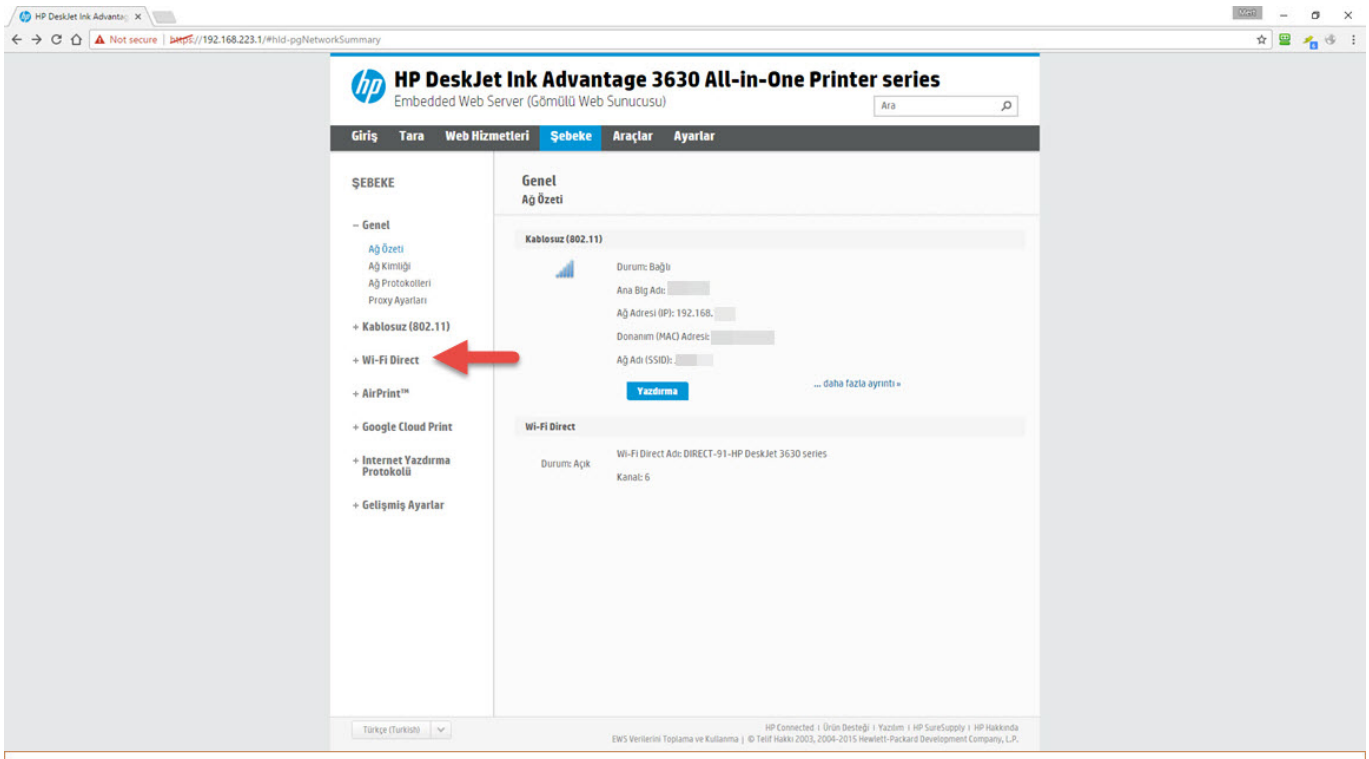
The basic function of the HP Scanner Thief tool is to make a request to the /eSCL/ScannerStatus page to check the status of the scanner and, if the JobUuid value is different from the previous value, to send a request to start the scanning process on the /eSCL/ScanJobs page and then download the resulting document from the /eSCL/ScanJobs/[uuid]/NextDocument page.

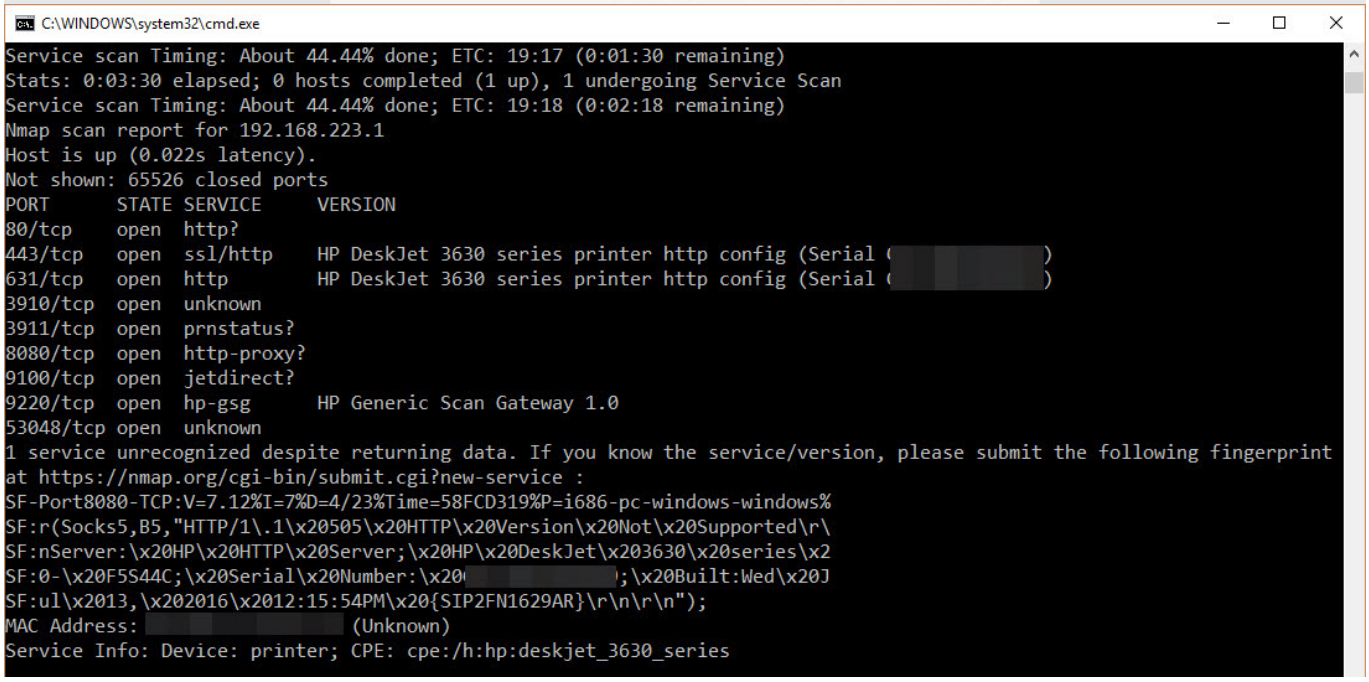




With the HP Scanner Thief tool, if a process is carried out on the scanner and the scanned document is not physically taken from the printer within 20 seconds, it is possible for the document to be digitally stolen. Therefore, it is very important to change the default Wi-Fi Direct password to a strong one from the management interface!

The lesson we should take away from this text and study is that when we purchase devices today, we should not only evaluate them in terms of price and performance, but also in terms of security. And after buying it, we should not just rely on the easy setup steps provided by the manufacturer, but also ensure its security by implementing a strong password, disabling unnecessary services and so on before including the device in our home or work network.





Hope to see you in the following articles.