Security Sidebar: My Printer Did What?!?

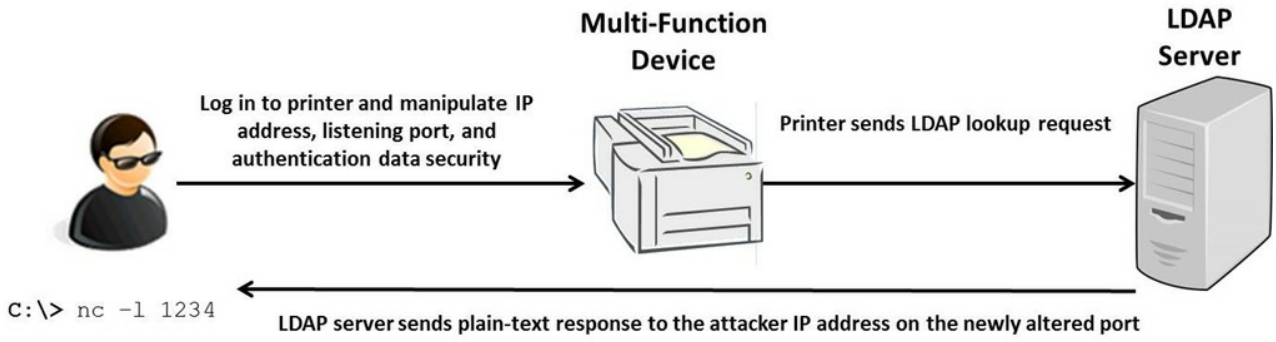
John Wagnon, 2014-18-08

Remember back in the good old days when a printer was just a printer? Well, that isn't reality any more. Printers have morphed from basic dot-matrix machines connected via parallel cable to fully-networked, multi-function devices on your network. Gone are the days of simply plugging in a USB to your work computer and printing on your own personal device. Now, it seems that everyone is using a complex, muti-function device that can print, scan, email, copy, fax, etc. And why not, right? If you can do all that stuff with one super-cool machine, there's no need to have tons of personal printers, scanners, copiers all over the place.

But as is the case with many things, the more functionality you introduce, the more vulnerabilities you expose. Companies purchase these high-end, expensive devices for several reasons. Like I mentioned above, the expensive ones are fully networked and offer lots of features that would otherwise require several individual machines. And, the higher-end machines typically offer the best quality in printing, copying, and scanning. In fact, if a company is only interested in high quality print, that company will likely be forced to purchase the fully networked device whether they need all the extra bells and whistles or not.

I recently watched a video presentation from a BSides event in Cleveland where Deral Heiland discussed different ways to hack these high-end printers. Deral did a great job, and I wanted to highlight one of the printer exploits he discussed...known as the LDAP Pass-Back-Attack.

The first step in this LDAP Pass-Back-Attack takes advantage of the fact that most printers still have the default settings for the admin username and password. There are several ways to gain access to the password if it has been changed, but as Deral mentions in his discussion, most printers use the default password. Once you log in to the printer, you should be able to change the IP address and service port, and many times you can change the authentication security so that the LDAP server will respond with passwords in plain text. Using an intercepting proxy like Burp Suite, you can capture and manipulate the LDAP lookup request data. When the LDAP server receives the manipulated lookup request, it will respond in plain text to the attacker's IP address on the newly-altered port number. The attacker can capture all the credentials using a tool like Netcat listener. Check it all out in the diagram below:



Once you have the LDAP credentials, you can test them on a legitimate LDAP server in the target network. If the LDAP server happens to be a Domain Controller, the attacker might just have himself some domain admin rights! What's more, many of these multi-function printers actually store user passwords in their address books, so an attacker could use this same attack to gain access to several user accounts directly from the printer.

Deral mentioned in his presentation that, in 2010, he gained access to Active Directory user accounts less than 10% of the time, and he rarely gained domain admin credentials using this attack. But, in 2014, he could gain access to Active Directory user accounts about 50% of the time, and this led to domain admin access almost 30% of the time. It seems we have stepped backward while stepping forward.

In order to guard against this attack, it's recommended to turn off automatic firmware upgrades for your multi-function devices, isolate printers by department, don't allow printers to have Internet access, and for crying out loud, change the default password!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com