Malware Analysis - Malicious Doc [Let's defend – Write-Up]

Analyze malicious .doc file

File: /root/Desktop/ChallengeFiles/factura.zip
Password: infected

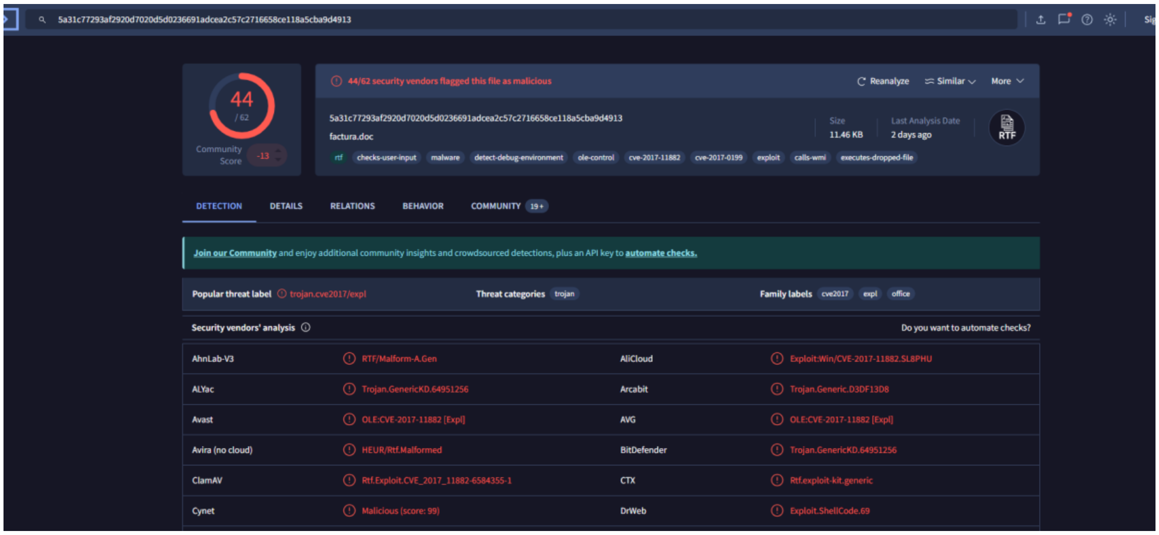
| Start Investigation

Q1: What type of exploit is running as a result of the relevant file running on the victim machine?

At the beginning of the investigation, I wanted to obtain the hash to analyze it in VirusTotal. Therefore, the first step I took was to execute the command `md5sum factura.doc` to calculate the hash, and the result was:

5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5cba9d4913

After that, I analyzed it in VirusTotal.



44/62 security vendors flagged this file as malicious

5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5cba9d4913
factura.doc

rtf checks-user-input malware detect-debug-environment ole-control cve-2017-11882 cve-2017-0199 exploit calls-wmi executes-dropped-file

Size: 11.46 KB
Last Analysis Date: 2 days ago

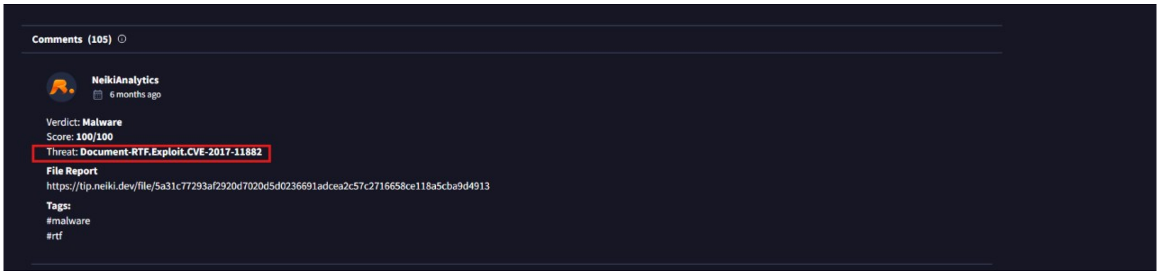
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.cve2017/expl
Threat categories: trojan
Family labels: cve2017 expl office

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	RTF/Malform-A.Gen	AliCloud	Exploit:Win/CVE-2017-11882.SL8PHU
ALYac	Trojan.GenericKD.64951256	Arcabit	Trojan.Generic.D3DF13D8
Avast	OLE:CVE-2017-11882 [Expl]	AVG	OLE:CVE-2017-11882 [Expl]
Avira (no cloud)	HEUR/Rtf.Malformed	BitDefender	Trojan.GenericKD.64951256
ClamAV	Rtf.Exploit.CVE_2017_11882-6584355-1	CTX	Rtf.exploit-kit.generic
Cynet	Malicious (score: 99)	DrWeb	Exploit.ShellCode.69



Comments (105)

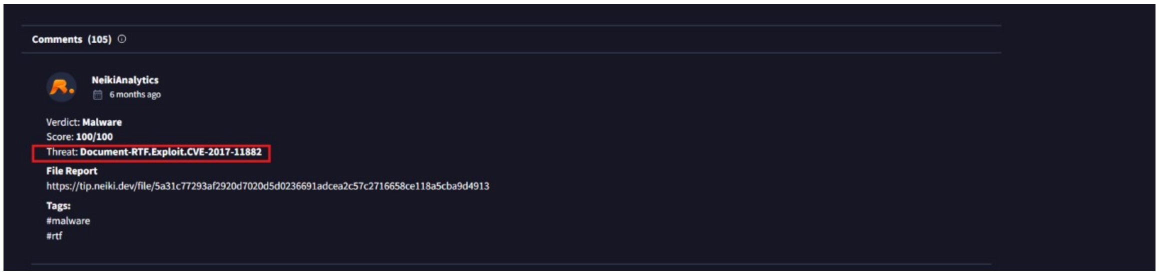
NeikiAnalytics
6 months ago

Verdict: Malware
Score: 100/100
Threat: Document-RTF.Exploit.CVE-2017-11882
File Report
https://tip.neiki.dev/file/5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5cba9d4913
Tags:
#malware
#rtf

Answer: rtf.exploit.

Q2: What is the relevant Exploit CVE code obtained as a result of the analysis?

The answer to the second question is also in the same image as the first question.



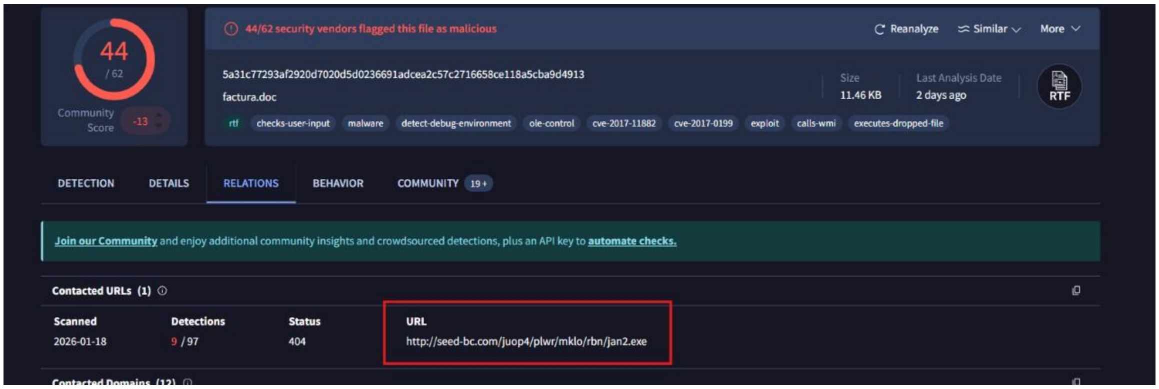
Comments (105)

NeikiAnalytics
6 months ago

Verdict: **Malware**
Score: **100/100**
Threat: **Document-RTF.Exploit.CVE-2017-11882**
File Report
https://tip.neiki.dev/file/5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5cba9d4913
Tags:
#malware
#rtf

Answer: cve-2017-11882.

Q3: What is the name of the malicious software downloaded from the internet as a result of the file running?



44/62 security vendors flagged this file as malicious

5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5cba9d4913
factura.doc

Size: 11.46 KB
Last Analysis Date: 2 days ago

rtf · checks-user-input · malware · detect-debug-environment · ole-control · cve-2017-11882 · cve-2017-0199 · exploit · calls-wmi · executes-dropped-file

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

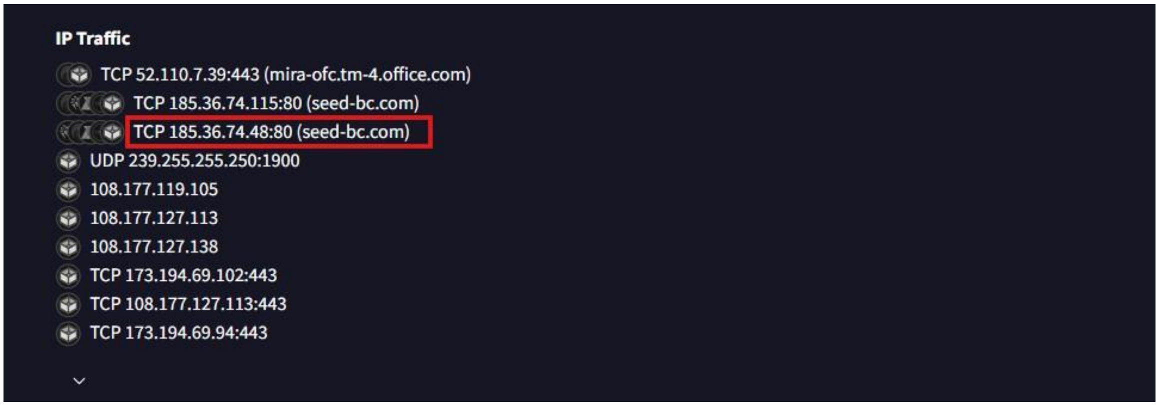
Contacted URLs (1)

Scanned	Detections	Status	URL
2026-01-18	9 / 97	404	http://seed-bc.com/juop4/plwr/mklo/rbn/jan2.exe

Contacted Domains (12)

Answer: jan2.exe.

Q4: What is the IP address and port information it communicates with?



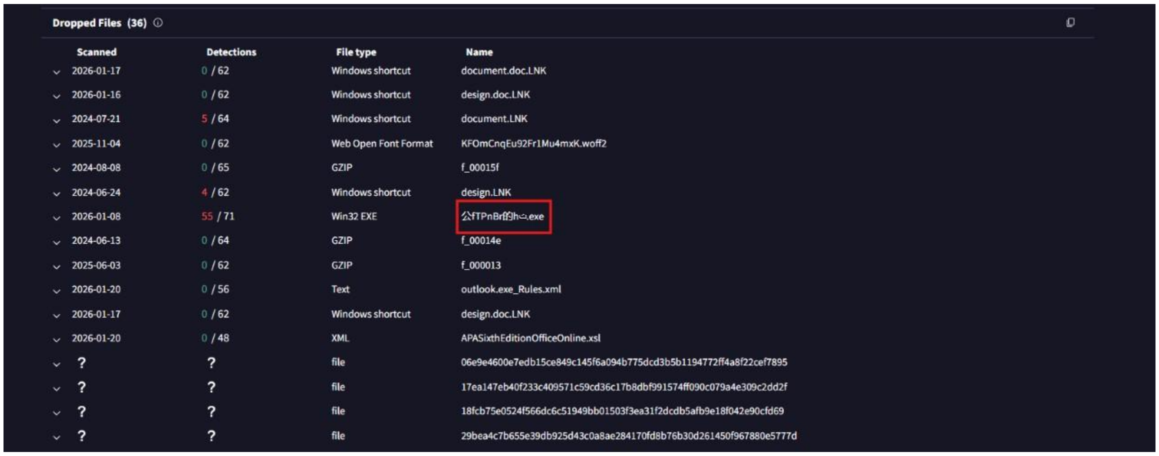
IP Traffic

TCP 52.110.7.39:443 (mira-ofc.tm-4.office.com)
TCP 185.36.74.115:80 (seed-bc.com)
TCP 185.36.74.48:80 (seed-bc.com)
UDP 239.255.255.250:1900
108.177.119.105
108.177.127.113
108.177.127.138
TCP 173.194.69.102:443
TCP 108.177.127.113:443
TCP 173.194.69.94:443

From Behavior ---> IP Traffic i Found the answer

Answer: 185.36.74.48:80.

Q5: What is the exe name it drops to disk after it runs?

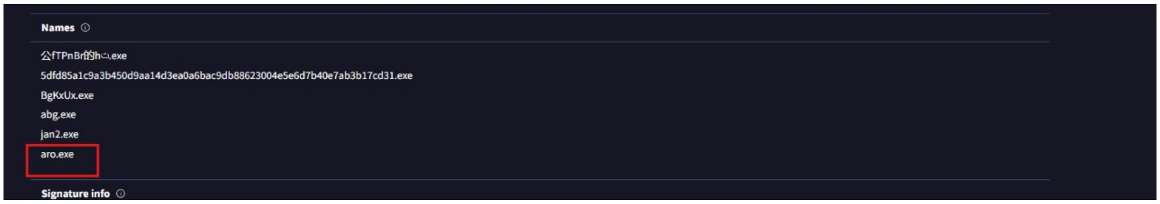


Dropped Files (36)

Scanned	Detections	File type	Name
2026-01-17	0 / 62	Windows shortcut	document.doc.LNK
2026-01-16	0 / 62	Windows shortcut	design.doc.LNK
2024-07-21	5 / 64	Windows shortcut	document.LNK
2025-11-04	0 / 62	Web Open Font Format	KFOmCnqEu92Fr1Mu4mxK.woff2
2024-08-08	0 / 65	GZIP	f_00015f
2024-06-24	4 / 62	Windows shortcut	design.LNK
2026-01-08	55 / 71	Win32 EXE	公fTPnBr的hت.exe
2024-06-13	0 / 64	GZIP	f_00014e
2025-06-03	0 / 62	GZIP	f_000013
2026-01-20	0 / 56	Text	outlook.exe_Rules.xml
2026-01-17	0 / 62	Windows shortcut	design.doc.LNK
2026-01-20	0 / 48	XML	APASixthEditionOfficeOnline.xsl
?	?	file	06e9e4600e7edb15ce849c145f6a094b775dcd3b5b1194772ff4a8f22cef7895
?	?	file	17ea147eb40f233c409571c59cd36c17b8dbf991574ff090c079a4e309c2dd2f
?	?	file	18fcb75e0524f566dc6c51949bb01503f3ea31f2dcdb5afb9e18f042e90cfd69
?	?	file	29bea4c7b655e39db925d43c0a8ae284170fd8b76b30d261450f967880e5777d

I checked the Dropped Files ansd i saw a file named.

公fTPnBr的h.تexe



Names

公fTPnBr的hت.exe
5dfd85a1c9a3b450d9aa14d3ea0a6bac9db88623004e5e6d7b40e7ab3b17cd31.exe
BgKxUx.exe
abg.exe
jan2.exe
aro.exe

Signature info

And I searched for the file and the I found the answer

Answer: aro.exe.

Summary

This lab helped me understand how hackers use Word documents to trigger exploits and infect systems. I learned how to track the download of malicious software, identify the IP addresses they communicate with, and find the hidden files they drop on the computer to stay active.