Rayan Alharbi

Rockford University

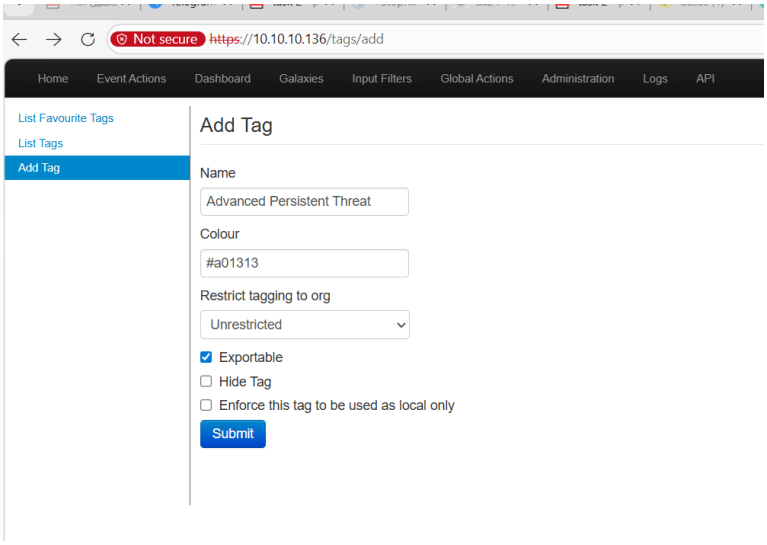
5/4/2026

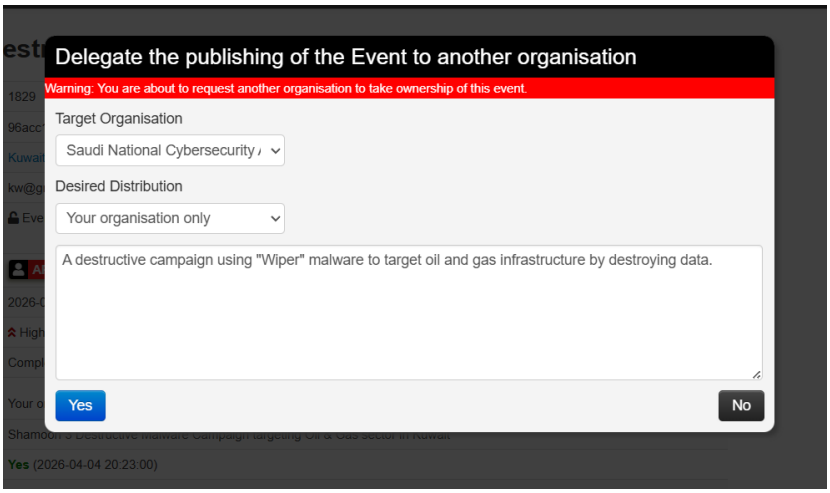
Introduction:

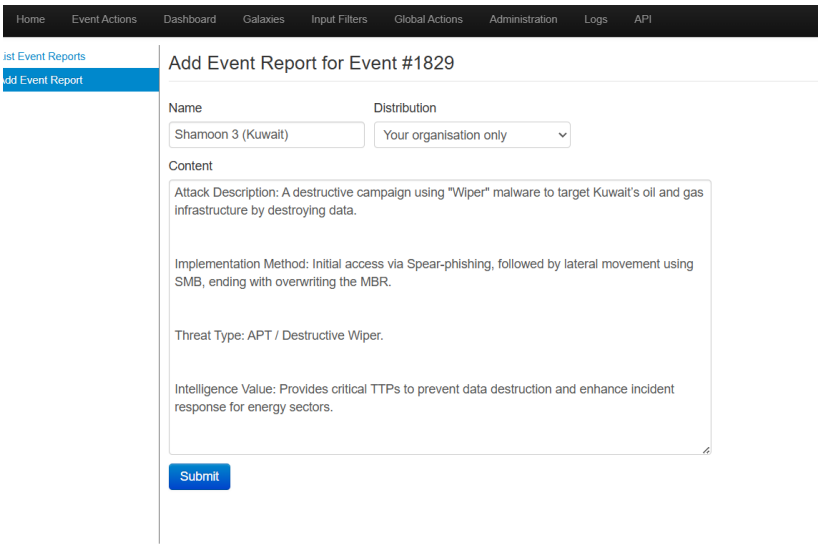
This project simulates a Cyber Threat Intelligence (CTI) environment using MISP, TheHive, and Cortex platforms. The goal of this project is to simulate real-world cyber threat intelligence operations including threat data collection, event creation, IOC analysis, threat investigation, and incident response. Multiple organizations were created to simulate intelligence sharing between countries and organizations. Threat events were created based on real-world APT campaigns and malware attacks, and indicators of compromise were analyzed using Cortex analyzers. The project demonstrates the integration between MISP for threat intelligence, TheHive for incident response, and Cortex for automated analysis.

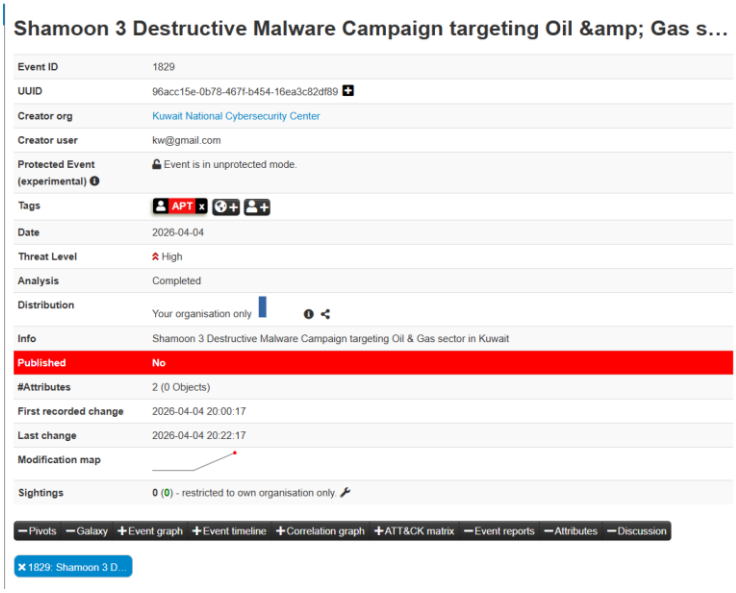
Event 1 – Shamoon Malware (Kuwait):

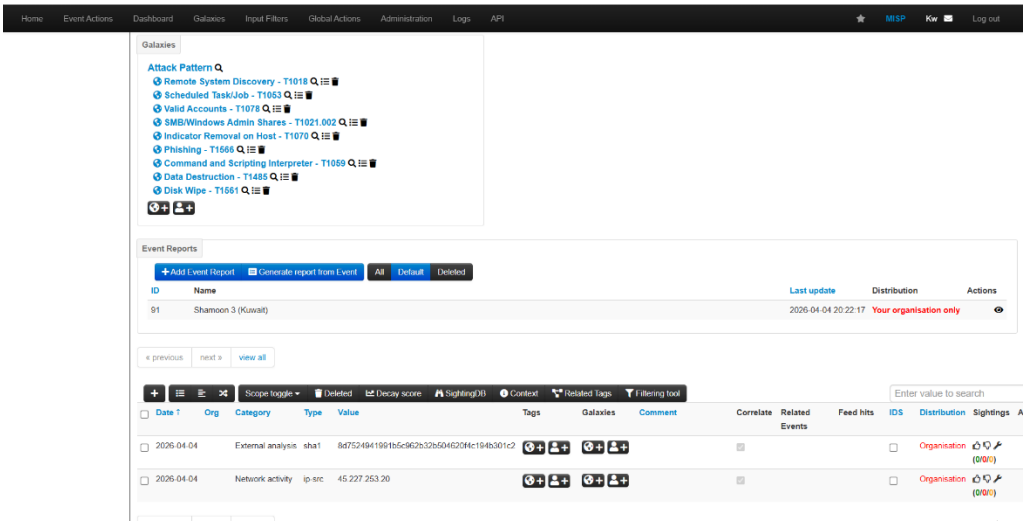
This event represents a destructive malware campaign known as Shamoon that targeted oil and gas infrastructure in Kuwait. Shamoon is a destructive wiper malware that deletes data and damages systems. The attack started with spear phishing emails and later moved laterally inside the network using SMB. The malware overwrote the Master Boot Record and destroyed system data. This event demonstrates destructive malware campaigns targeting critical infrastructure.




Delegate the publishing of the Event to another organisation
Warning: You are about to request another organisation to take ownership of this event.
Target Organisation
Saudi National Cybersecurity
Desired Distribution
Your organisation only
A destructive campaign using "Wiper" malware to target oil and gas infrastructure by destroying data.
Yes
No
Yes (2026-04-04 20:23:00)


Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Administration
Logs
API
Add Event Report
Add Event Report for Event #1829
Name
Shamoon 3 (Kuwait)
Distribution
Your organisation only
Content
Attack Description: A destructive campaign using "Wiper" malware to target Kuwait's oil and gas infrastructure by destroying data.
Implementation Method: Initial access via Spear-phishing, followed by lateral movement using SMB, ending with overwriting the MBR.
Threat Type: APT / Destructive Wiper.
Intelligence Value: Provides critical TTPs to prevent data destruction and enhance incident response for energy sectors.
Submit


Shamoon 3 Destructive Malware Campaign targeting Oil & Gas s...
Event ID 1829
UUID 96acc15e-0b78-467f-b454-16ea3c82df89
Creator org Kuwait National Cybersecurity Center
Creator user kw@gmail.com
Protected Event (experimental) Event is in unprotected mode.
Tags APT
Date 2026-04-04
Threat Level High
Analysis Completed
Distribution Your organisation only
Info Shamoon 3 Destructive Malware Campaign targeting Oil & Gas sector in Kuwait
Published No
#Attributes 2 (0 Objects)
First recorded change 2026-04-04 20:00:17
Last change 2026-04-04 20:22:17
Modification map
Sightings 0 (0) - restricted to own organisation only.
Pivots Galaxy Event graph Event timeline Correlation graph ATT&CK matrix Event reports Attributes Discussion
1829: Shamoon 3 D...



Users index

Click **here** to reset the API keys of all sync and org admin users in one shot. This will also automatically inform them of their new API keys.

« previous | next »

All | Active | Disabled

Enter value to search | Filter

ID	Org	Role	Email	Event alert	Contact alert	PGP Key	NIDS SID	Terms Accepted	Last Login	Created	Disabled	Actions
26	Kuwait National Cybersecurity Center	Org Admin	kw@gmail.com	✔	✔	✖	7086646	✖	2026-04-04 19:55:14	2026-04-01 10:51:52	✖	
27	Kuwait National Cybersecurity Center	Publisher	kw1@gmail.com	✔	✔	✖	2793466	✖	2026-04-02 10:39:56	2026-04-01 10:52:34	✖	
28	Kuwait National Cybersecurity Center	Read Only	kw2@gmail.com	✔	✔	✖	6299090	✖	Never	2026-04-01 10:53:19	✖	
31	Kuwait National Cybersecurity Center	User	kw0@gmail.com	✔	✔	✖	2289191	✔	Never	2026-04-02 10:28:39	✖	

Delegation index

« previous | next »

Pending | Issued

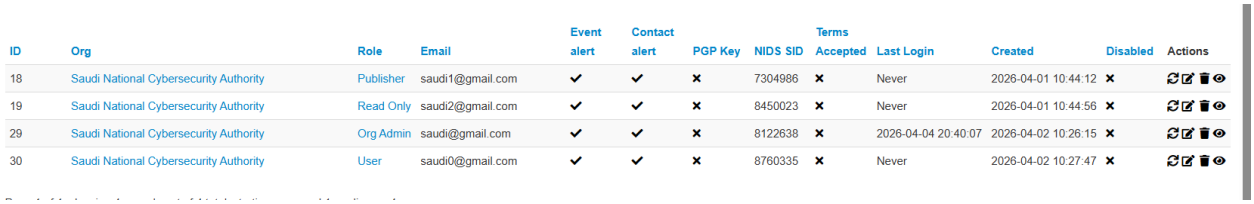
Enter value to search | Filter

Id	Requester	Recipient	Event id	Event info	Message
6	Kuwait National Cybersecurity Center	Saudi National Cybersecurity Authority	1829	Shamoon 3 Destructive Malware Campaign targeting Oil & Gas sector in Kuwait	A destructive campaign using "Wiper" malware to target oil and gas infrastructure by destroying data.

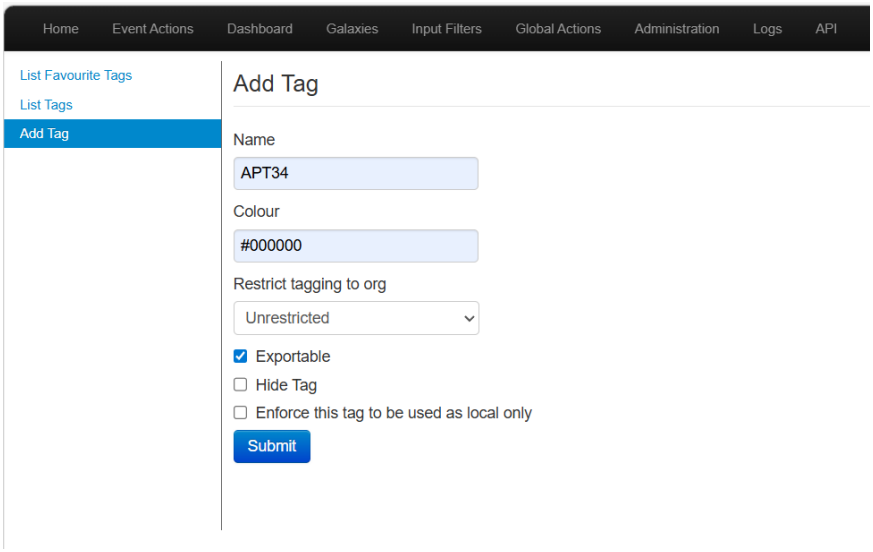
Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

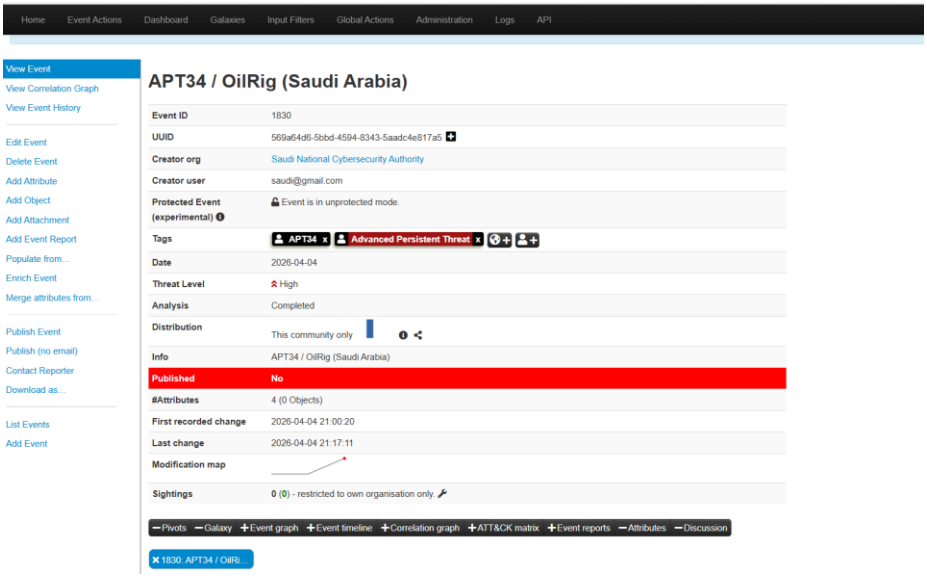
Event 2 – APT34 OilRig (Saudi Arabia):

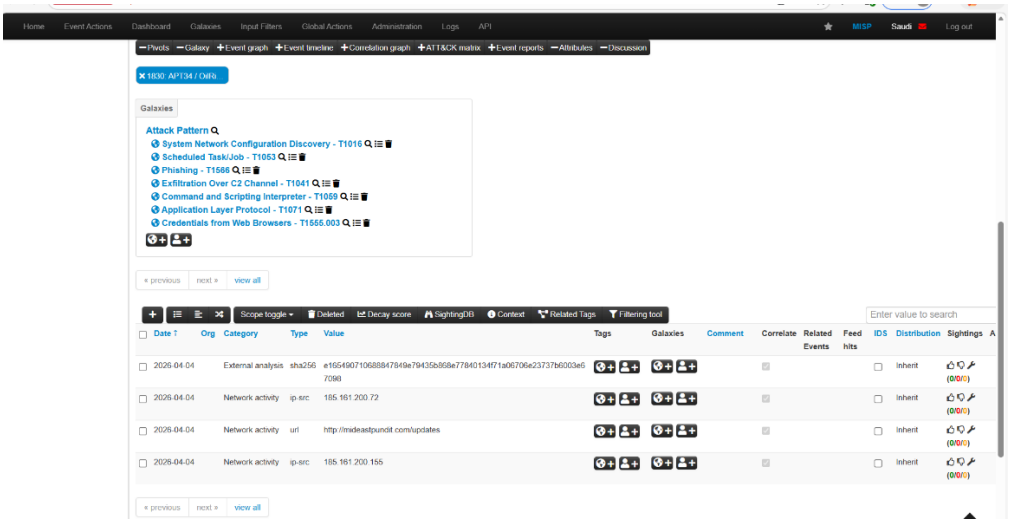
This event represents an Advanced Persistent Threat campaign known as APT34 (OilRig), which targeted government organizations in Saudi Arabia. The attackers used spear phishing emails with malicious attachments to gain initial access. After gaining access, the attackers used PowerShell backdoors and command and control communication to maintain persistence and steal sensitive information. This event demonstrates cyber espionage operations conducted by APT groups.

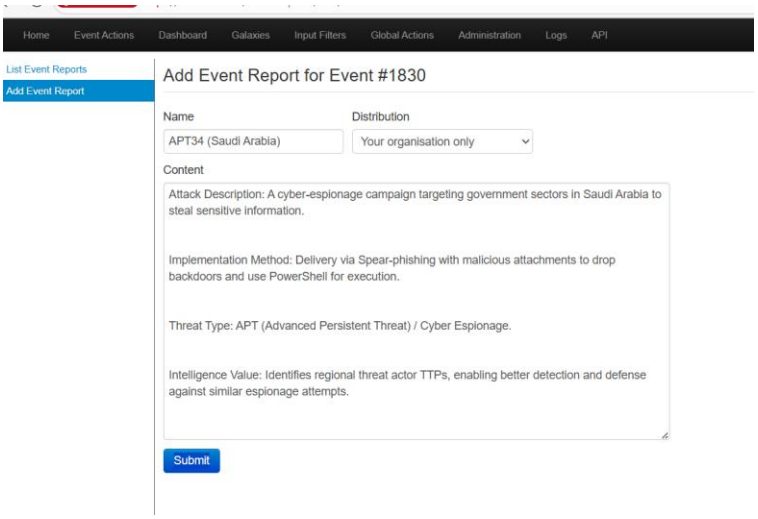


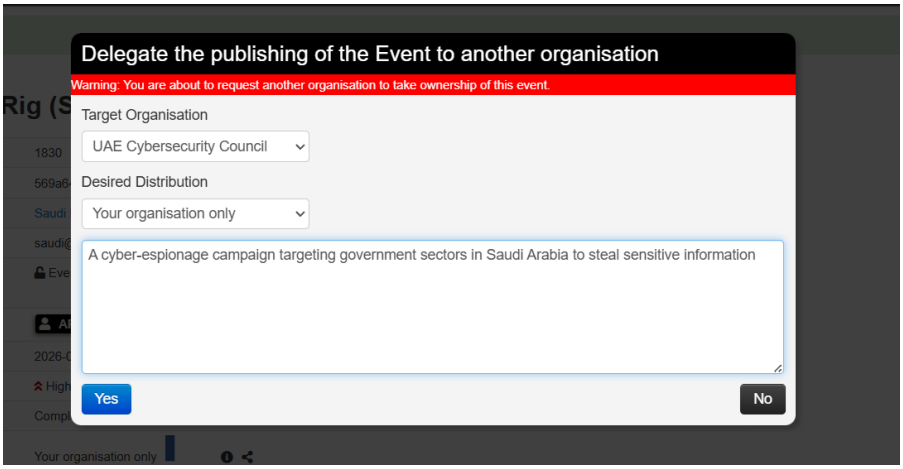
ID	Org	Role	Email	Event alert	Contact alert	PGP Key	NIDS SID	Terms Accepted	Last Login	Created	Disabled	Actions
18	Saudi National Cybersecurity Authority	Publisher	saudi1@gmail.com	✓	✓	✗	7304986	✗	Never	2026-04-01 10:44:12	✗	
19	Saudi National Cybersecurity Authority	Read Only	saudi2@gmail.com	✓	✓	✗	8450023	✗	Never	2026-04-01 10:44:56	✗	
29	Saudi National Cybersecurity Authority	Org Admin	saudi@gmail.com	✓	✓	✗	8122638	✗	2026-04-04 20:40:07	2026-04-02 10:26:15	✗	
30	Saudi National Cybersecurity Authority	User	saudi0@gmail.com	✓	✓	✗	8760335	✗	Never	2026-04-02 10:27:47	✗	




Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Administration
Logs
API
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Contact Reporter
Download as...
List Events
Add Event
APT34 / OilRig (Saudi Arabia)
Event ID 1830
UUID 569a64d6-5bbd-4594-8343-5aadc4e817a5
Creator org Saudi National Cybersecurity Authority
Creator user saudi@gmail.com
Protected Event (experimental) Event is in unprotected mode.
Tags APT34 Advanced Persistent Threat
Date 2026-04-04
Threat Level High
Analysis Completed
Distribution This community only
Info APT34 / OilRig (Saudi Arabia)
Published No
#Attributes 4 (0 Objects)
First recorded change 2026-04-04 21:00:20
Last change 2026-04-04 21:17:11
Modification map
Sightings 0 (0) - restricted to own organisation only.
Pivots Galaxy Event graph Event timeline Correlation graph ATT&CK matrix Event reports Attributes Discussion
1830: APT34 / OilRi...


Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Administration
Logs
API
MISP
Saudi
Log out
Pivots Galaxy Event graph Event timeline Correlation graph ATT&CK matrix Event reports Attributes Discussion
1830: APT34 / OilRi
Galaxies
Attack Pattern
System Network Configuration Discovery - T1016
Scheduled Task/Job - T1053
Phishing - T1566
Exfiltration Over C2 Channel - T1041
Command and Scripting Interpreter - T1059
Application Layer Protocol - T1071
Credentials from Web Browsers - T1555.003
« previous next » view all
Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool
Enter value to search
Date Org Category Type Value Tags Galaxies Comment Correlate Related Events Feed hits IDS Distribution Sightings
2026-04-04 External analysis sha256 e165490710688847849e79435b868e7784013 4f71a06706e23737b6003e670f90 Inherit (0/0/0)
2026-04-04 Network activity ip-src 185.161.209.72 Inherit (0/0/0)
2026-04-04 Network activity url http://mideastpundit.com/updates Inherit (0/0/0)
2026-04-04 Network activity ip-src 185.161.209.155 Inherit (0/0/0)
« previous next » view all





Delegation index

« previous next »

Pending Issued

Enter value to search Filter

Id	Requester	Recipient	Event id	Event info	Message
7	Saudi National Cybersecurity Authority	UAE Cybersecurity Council	1830	APT34 / OilRig (Saudi Arabia)	A cyber-espionage campaign targeting government sectors in Saudi Arabia to steal sensitive information

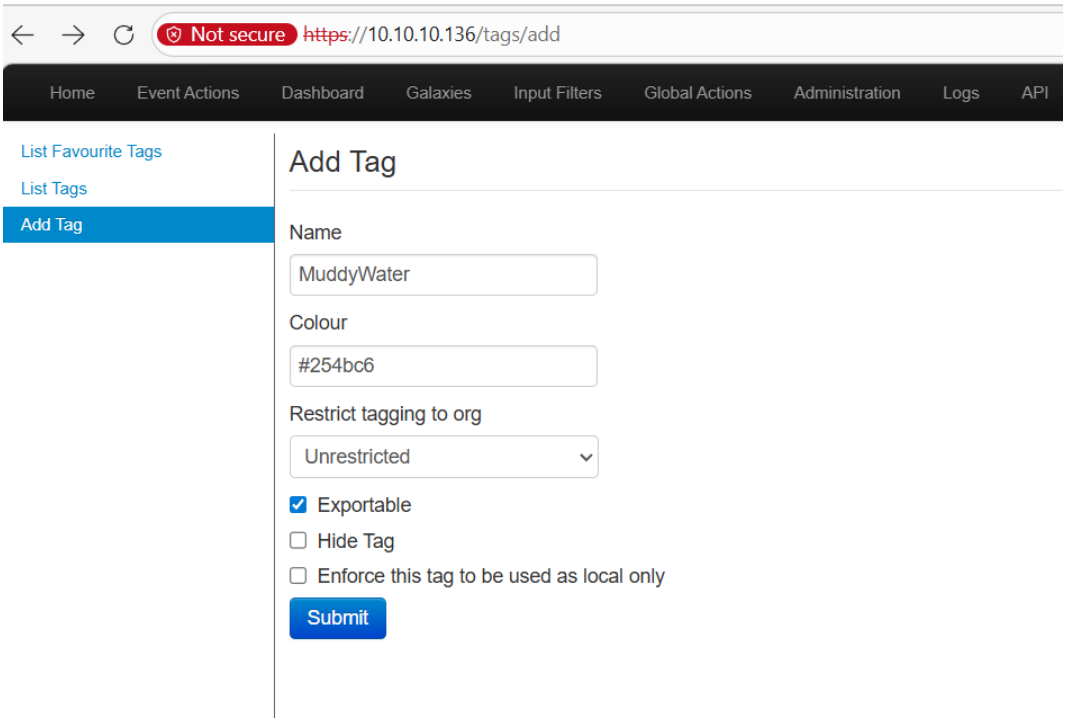
Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

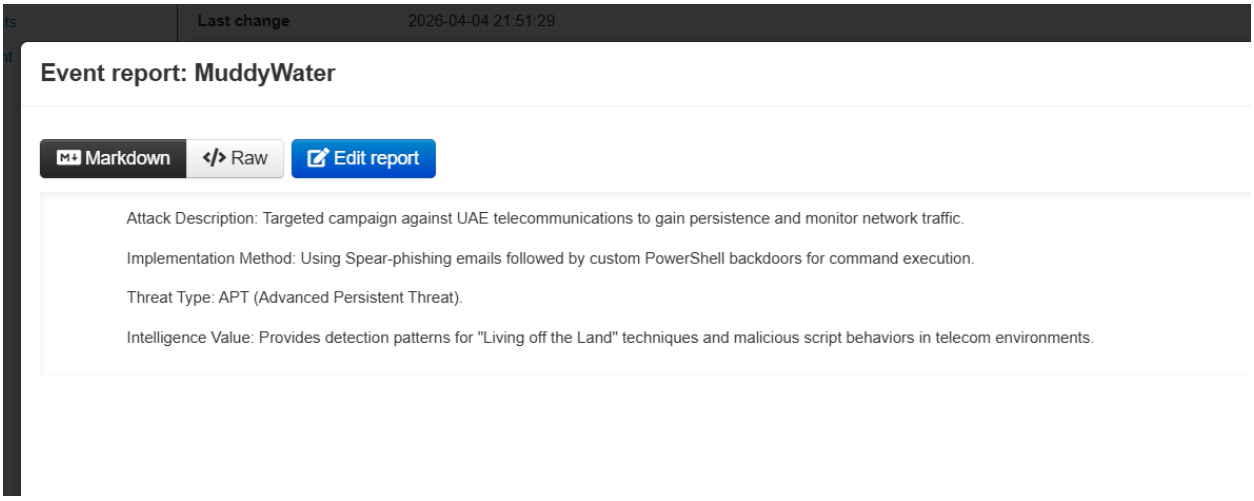
« previous next »

Event 3 – MuddyWater (UAE):

This event represents the MuddyWater APT group campaign targeting telecommunications organizations in the UAE. The attackers used spear phishing emails and malicious PowerShell scripts to gain access and maintain persistence in the network. The attackers used living-off-the-land techniques and PowerShell tools to avoid detection and monitor network traffic. This campaign represents cyber espionage and long-term persistence attacks.

ID	Org	Role	Email	Event alert	Contact alert	PGP Key	NIDS SID	Terms Accepted	Last Login	Created	Disabled	Actions
23	UAE Cybersecurity Council	Org Admin	ae@gmail.com	✔	✔	✖	4725598	✖	2026-04-04 21:30:55	2026-04-01 10:48:37	✖	
24	UAE Cybersecurity Council	Publisher	ae1@gmail.com	✔	✔	✖	1839245	✖	Never	2026-04-01 10:49:22	✖	
25	UAE Cybersecurity Council	Read Only	ae2@gmail.com	✔	✔	✖	5537895	✖	Never	2026-04-01 10:49:47	✖	
33	UAE Cybersecurity Council	User	ae0@gmail.com	✔	✔	✖	2659050	✖	Never	2026-04-02 10:32:27	✖	


Not secure https://10.10.10.136/tags/add
Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Administration
Logs
API
List Favourite Tags
List Tags
Add Tag
Add Tag
Name
MuddyWater
Colour
#254bc6
Restrict tagging to org
Unrestricted
Exportable
Hide Tag
Enforce this tag to be used as local only
Submit


Last change
2026-04-04 21:51:29
Event report: MuddyWater
Markdown
Raw
Edit report
Attack Description: Targeted campaign against UAE telecommunications to gain persistence and monitor network traffic.
Implementation Method: Using Spear-phishing emails followed by custom PowerShell backdoors for command execution.
Threat Type: APT (Advanced Persistent Threat).
Intelligence Value: Provides detection patterns for "Living off the Land" techniques and malicious script behaviors in telecom environments.

MuddyWater (UAE)

Event ID	1831
UUID	d1f006a2-5de7-4b2f-a03d-2d06dced41a2
Creator org	UAE Cybersecurity Council
Creator user	ae@gmail.com
Protected Event (experimental)	Event is in unprotected mode.
Tags	MuddyWater x APT x
Date	2026-04-04
Threat Level	High
Analysis	Completed
Distribution	Your organisation only
Info	MuddyWater (UAE)
Published	**No**
#Attributes	3 (0 Objects)
First recorded change	2026-04-04 21:39:56
Last change	2026-04-04 21:51:29
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Pivots | Galaxy | Event graph | Event timeline | Correlation graph | ATT&CK matrix | Event reports | Attributes | Discussion

Galaxies

Attack Pattern

- Spearphishing Attachment - T1566.001
- System Network Configuration Discovery - T1016
- Scheduled Task/Job - T1053
- Application Layer Protocol - T1071
- PowerShell - T1086
- Deobfuscate/Decode Files or Information - T1140

Event Reports

Add Event Report | Generate report from Event | All | Default | Deleted

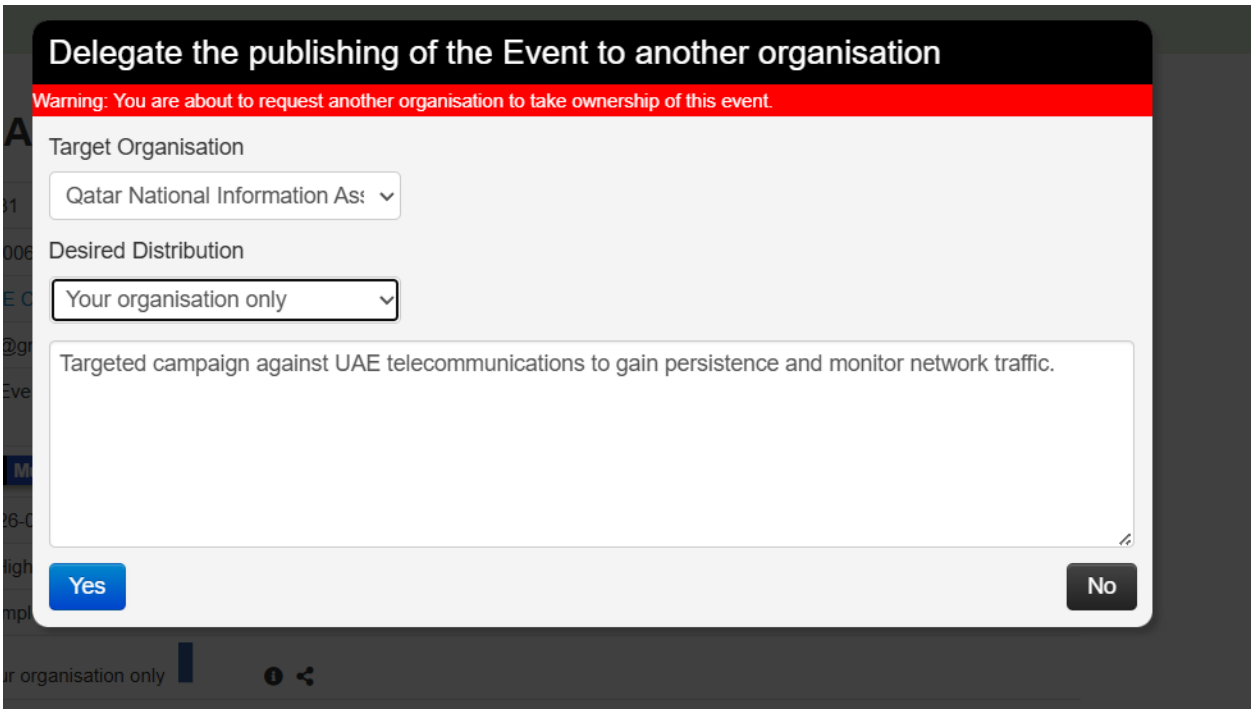
ID	Name	Last update	Distribution	Actions
93	MuddyWater	2026-04-04 21:51:29	Your organisation only	

« previous | next » | view all

Scope toggle | Deleted | Decay score | SightingDB | Context | Related Tags | Filtering tool

Enter value to search

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings
2026-04-04		Network activity	url	https://sh-link.org/api/v1/update								Inherit	(0/0/0)
2026-04-04		Network activity	ip-src	91.235.129.57								Inherit	(0/0/0)
2026-04-04		External analysis	md5	8e40f279165681c5fcc3604f32997637								Inherit	(0/0/0)



Delegation index

« previous next »

Pending Issued

Enter value to search Filter

Id	Requester	Recipient	Event id	Event info	Message
8	UAE Cybersecurity Council	Qatar National Information Assurance	1831	MuddyWater (UAE)	Targeted campaign against UAE telecommunications to gain persistence and monitor network traffic.

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

« previous next »

Event 4 – Bahamut Campaign (Qatar):

This event represents the Bahamut cyber espionage campaign targeting financial institutions in Qatar. The attackers used fake banking websites and malicious applications to steal user credentials and sensitive financial information. The campaign involved social engineering, phishing websites, and spyware tools to monitor financial communications. This campaign represents credential harvesting and cyber espionage operations.

ID	Org	Role	Email	Event alert	Contact alert	PGP Key	NIDS SID	Terms Accepted	Last Login	Created	Disabled	Actions
20	Qatar National Information Assurance	admin	qatar@gmail.com	✔	✔	✖	2958439	✔	2026-04-04 21:57:43	2026-04-01 10:46:03	✖	
21	Qatar National Information Assurance	Publisher	qatar1@gmail.com	✔	✔	✖	7311884	✖	Never	2026-04-01 10:47:08	✖	
22	Qatar National Information Assurance	Read Only	qatar2@gmail.com	✔	✔	✖	4402754	✖	Never	2026-04-01 10:47:36	✖	
32	Qatar National Information Assurance	admin	qatar0@gmail.com	✔	✔	✖	5722254	✔	Never	2026-04-02 10:29:30	✖	

t Favourite Tags

t Tags

d Tag

Add Tag

Name

Bahamut Campaign

Colour

#2c9e21

Restrict tagging to org

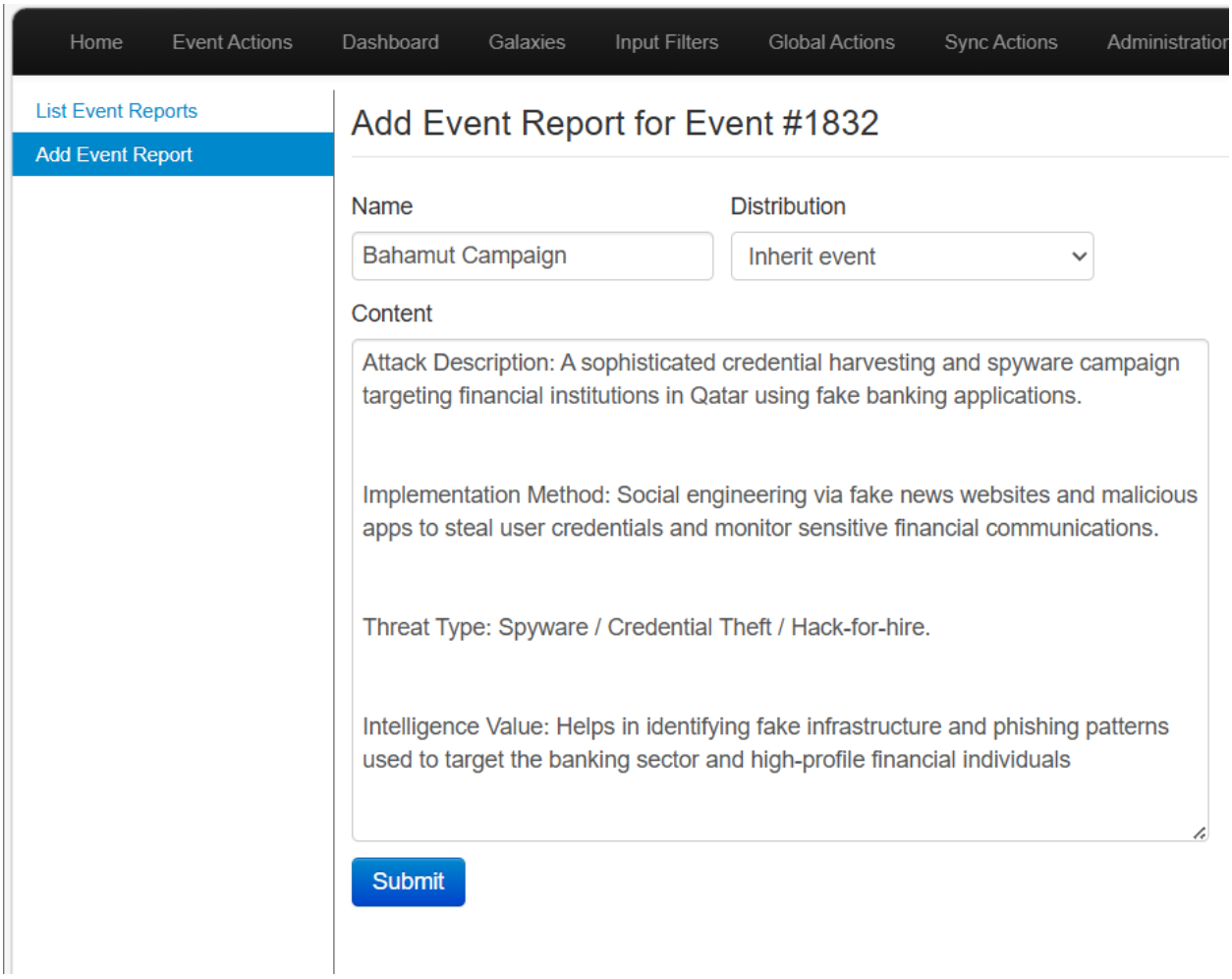
Unrestricted

Restrict tagging to user

Unrestricted

- [x] Exportable
- [ ] Hide Tag
- [ ] Enforce this tag to be used as local only

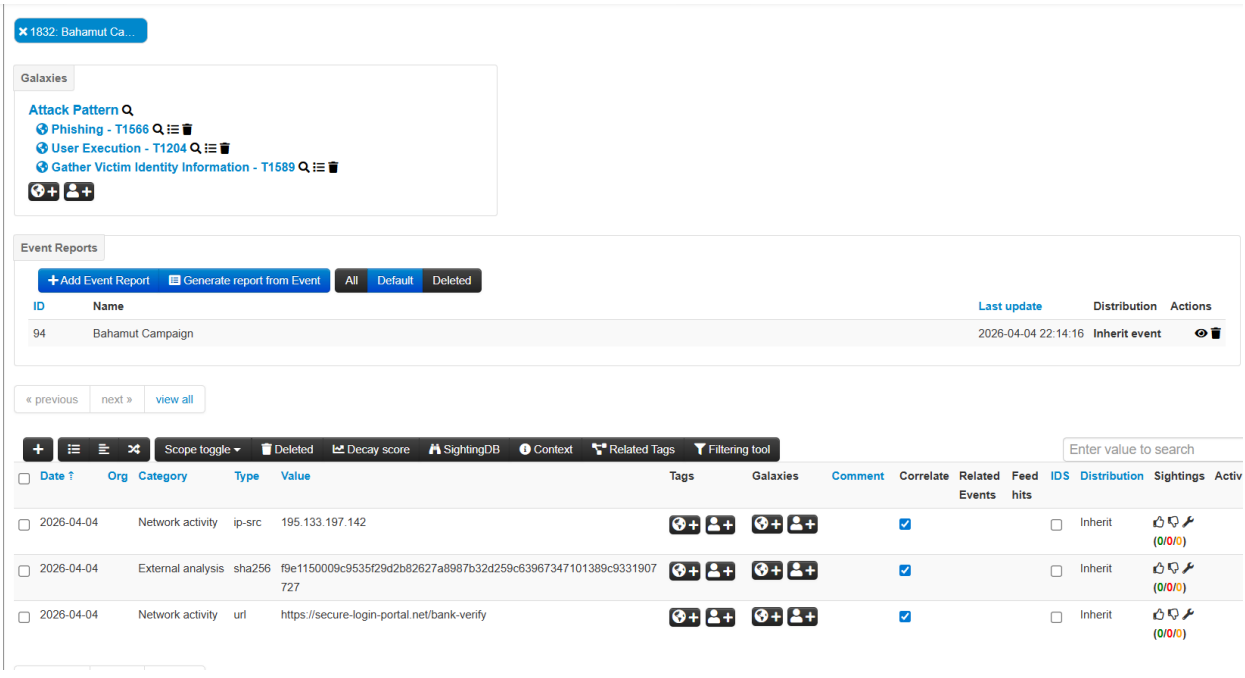
Submit

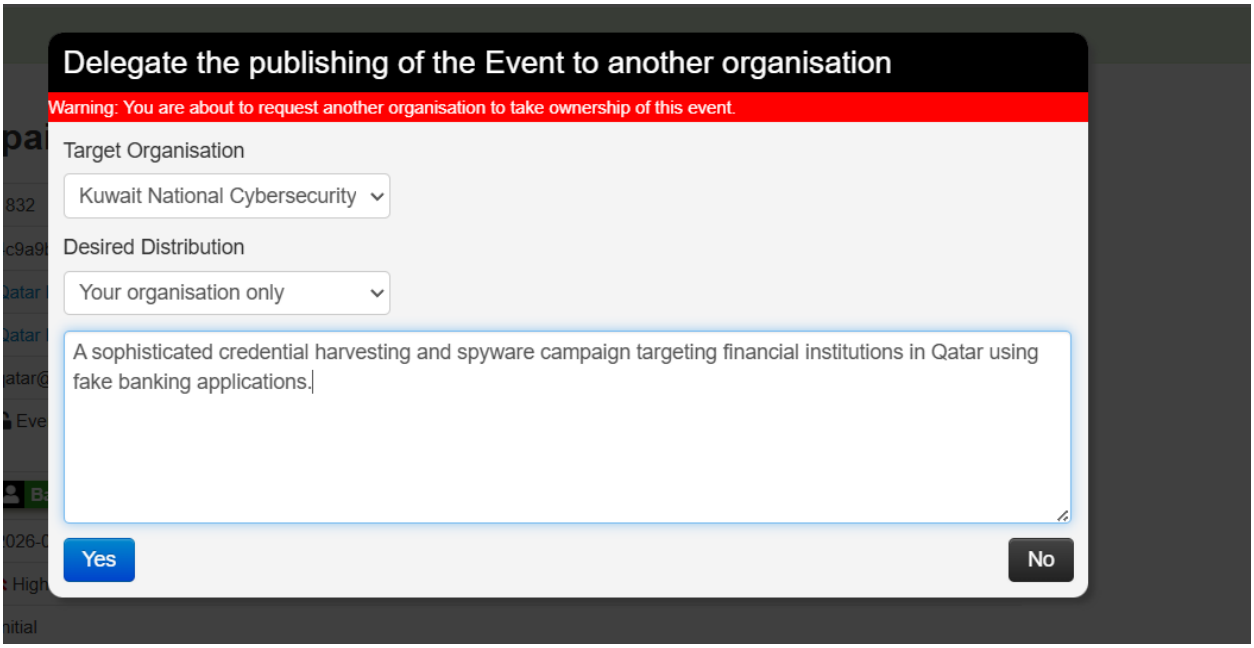

Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
List Event Reports
Add Event Report
Add Event Report for Event #1832
Name
Bahamut Campaign
Distribution
Inherit event
Content
Attack Description: A sophisticated credential harvesting and spyware campaign targeting financial institutions in Qatar using fake banking applications.
Implementation Method: Social engineering via fake news websites and malicious apps to steal user credentials and monitor sensitive financial communications.
Threat Type: Spyware / Credential Theft / Hack-for-hire.
Intelligence Value: Helps in identifying fake infrastructure and phishing patterns used to target the banking sector and high-profile financial individuals
Submit

Bahamut Campaign (Qatar)

Event ID	1832
UUID	4c9a9b0c-16ba-4653-9f83-6f0f6b545814
Creator org	Qatar National Information Assurance
Owner org	Qatar National Information Assurance
Creator user	qatar@gmail.com
Protected Event (experimental)	Event is in unprotected mode.
Tags	Bahamut Campaign x APT x
Date	2026-04-04
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Bahamut Campaign (Qatar)
Published	**No**
#Attributes	3 (0 Objects)
First recorded change	2026-04-04 22:11:21
Last change	2026-04-04 22:19:02
Modification map	
Sightings	0 (0) - restricted to own organisation only.

−Pivots −Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix −Event reports −Attributes −Discussion

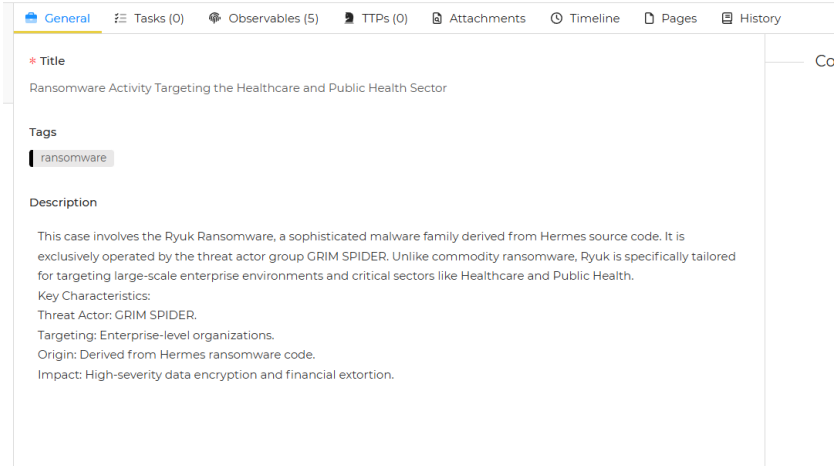


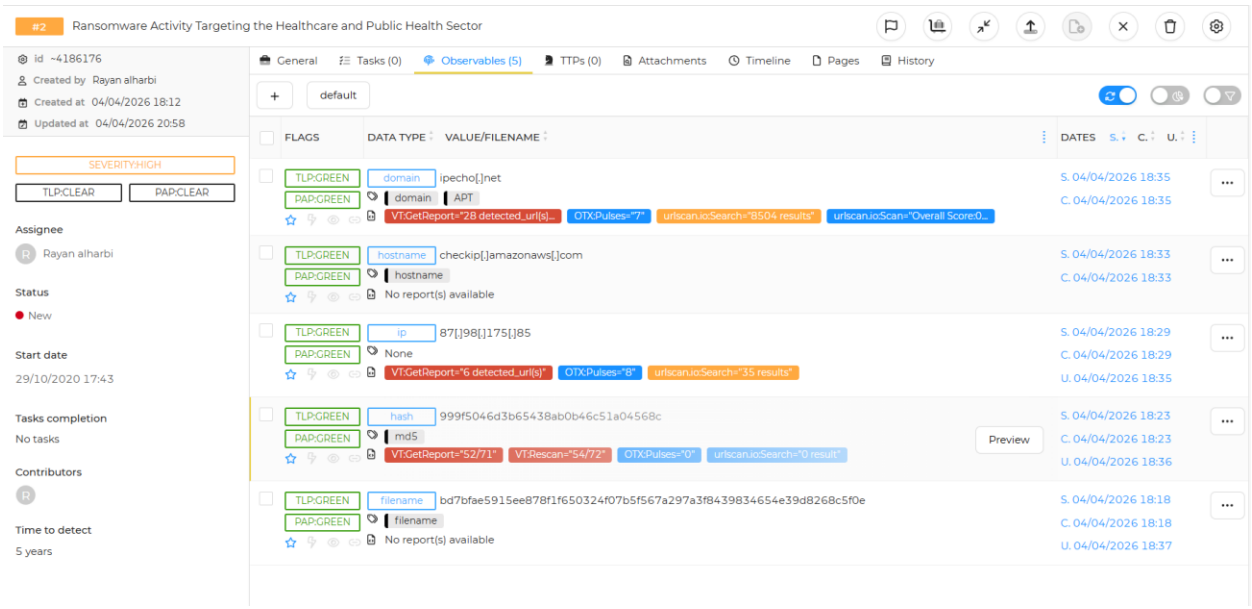

Delegate the publishing of the Event to another organisation
Warning: You are about to request another organisation to take ownership of this event.
Target Organisation
Kuwait National Cybersecurity
Desired Distribution
Your organisation only
A sophisticated credential harvesting and spyware campaign targeting financial institutions in Qatar using fake banking applications.
Yes
No

Task 2 – Threat Intelligence Analysis (Ryuk Ransomware):

In **Task 2**, a threat intelligence analysis was performed based on a **Ryuk Ransomware** event targeting the healthcare and public health sector. The investigation began by extracting indicators of compromise (IoCs) from **MISP**, including a malicious payload hash, C2 server IP addresses, and connectivity-check domains like ipecho.net. These indicators were imported into **TheHive** to manage the case.

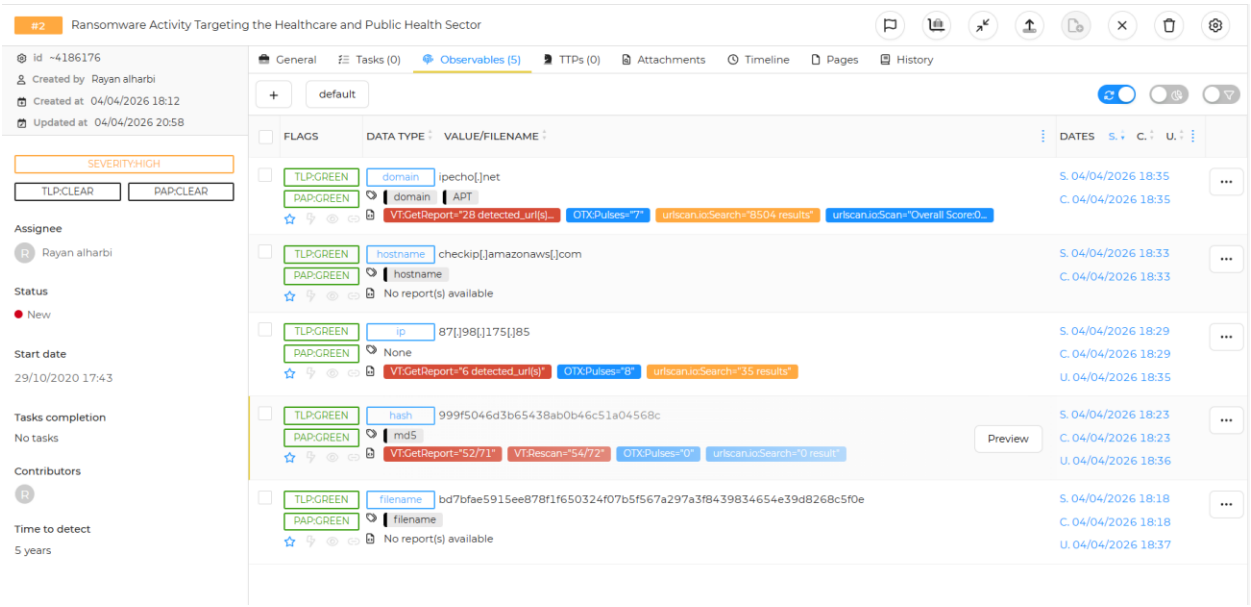
Using **Cortex**, the indicators were enriched through automated analyzers such as **VirusTotal**, **AlienVault OTX**, and **Censys**. The analysis revealed a high detection rate (**52/71** on VirusTotal) for the malware hash and confirmed that the IP address 87.98.175.85 was part of a known malicious infrastructure. The threat was attributed to the **GRIM SPIDER** group, and the final decision was to **Block** all indicators and initiate containment procedures to prevent data encryption and further lateral movement


General
Tasks (0)
Observables (5)
TTPs (0)
Attachments
Timeline
Pages
History
* Title
Ransomware Activity Targeting the Healthcare and Public Health Sector
Tags
ransomware
Description
This case involves the Ryuk Ransomware, a sophisticated malware family derived from Hermes source code. It is exclusively operated by the threat actor group GRIM SPIDER. Unlike commodity ransomware, Ryuk is specifically tailored for targeting large-scale enterprise environments and critical sectors like Healthcare and Public Health.
Key Characteristics:
Threat Actor: GRIM SPIDER.
Targeting: Enterprise-level organizations.
Origin: Derived from Hermes ransomware code.
Impact: High-severity data encryption and financial extortion.


#2
Ransomware Activity Targeting the Healthcare and Public Health Sector
id ~4186176
Created by Rayan alharbi
Created at 04/04/2026 18:12
Updated at 04/04/2026 20:58
SEVERITY:HIGH
TLP:CLEAR
PAP:CLEAR
Assignee
Rayan alharbi
Status
New
Start date
29/10/2020 17:43
Tasks completion
No tasks
Contributors
Time to detect
5 years
General
Tasks (0)
Observables (5)
TTPs (0)
Attachments
Timeline
Pages
History
default
FLAGS
DATA TYPE
VALUE/FILENAME
DATES
TLP:GREEN
PAP:GREEN
domain
ipecho[.]net
APT
VT:GetReport="28 detected_url(s)...
OTX:Pulses="7"
urlscan.io:Search="8504 results"
urlscan.io:Scan="Overall Score:0...
S. 04/04/2026 18:35
C. 04/04/2026 18:35
hostname
checkip[.]amazonaws[.]com
No report(s) available
S. 04/04/2026 18:33
C. 04/04/2026 18:33
ip
87[.]98[.]175[.]85
None
VT:GetReport="6 detected_url(s)"
OTX:Pulses="8"
urlscan.io:Search="35 results"
S. 04/04/2026 18:29
C. 04/04/2026 18:29
U. 04/04/2026 18:35
hash
999f5046d3b65438ab0b46c51a04568c
md5
VT:GetReport="52/71"
VT:Rescan="54/72"
OTX:Pulses="0"
urlscan.io:Search="0 result"
Preview
S. 04/04/2026 18:23
C. 04/04/2026 18:23
U. 04/04/2026 18:36
filename
bd7bfae5915ee878f1f650324f07b5f567a297a3f8439834654e39d8268c5f0e
No report(s) available
S. 04/04/2026 18:18
C. 04/04/2026 18:18
U. 04/04/2026 18:37

Task 3 – APT Incident Simulation (Emotet Attack):

In Task 3, an APT attack simulation was performed based on a phishing email attack containing a malicious Office document with a macro. When the user enabled macros, malware was downloaded and installed on the system. The malware established persistence, connected to a command and control server, and exfiltrated credentials and system information. Indicators of compromise such as IP address, domain, and malware hash were added to TheHive and analyzed using Cortex. The attack was mapped to MITRE ATT&CK techniques, and the final decision was to block the indicators and contain the threat.



Emotet Macro Malware Attack

Event ID	1833
UUID	34f24461-46d5-48aa-aad9-72a5ed950bf4
Creator org	Rayan111
Creator user	ryan1112015@gmail.com
Protected Event (experimental)	Event is in unprotected mode.
Tags	Remove tag — CZ x, APT x, Emotet x, Phishing x
Date	2026-04-05
Threat Level	High
Analysis	Completed
Distribution	Your organisation only
Info	Emotet Macro Malware Attack
Published	No
#Attributes	3 (0 Objects)
First recorded change	2026-04-05 02:06:46
Last change	2026-04-05 02:28:02
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Pivots | Galaxy | Event graph | Event timeline | Correlation graph | ATT&CK matrix | Event reports | Attributes | Discussion

1833: Emotet Macr...

Pivots | Galaxy | Event graph | Event timeline | Correlation graph | ATT&CK matrix | Event reports | Attributes | Discussion

1833: Emotet Macr...

Galaxies

Attack Pattern
- Registry Run Keys / Startup Folder - T1060
- Phishing - T1566
- Web Protocols - T1071.001
- Malicious File - T1204.002
- Exfiltration Over Web Service - T1567

Event Reports

Add Event Report | Generate report from Event | All | Default | Deleted

ID	Name	Last update	Distribution	Actions
96	Attack Stages	2026-04-05 02:26:16	Your organisation only	
95	Emotet Macro Malware Attack	2026-04-05 02:22:23	Inherit event	
98	Impact	2026-04-05 02:28:02	Your organisation only	
97	Spread Method	2026-04-05 02:27:38	Your organisation only	

« previous | next » | view all

Scope toggle | Deleted | Decay score | SightingDB | Context | Related Tags | Filtering tool | Enter value to search

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2026-04-05		External analysis	sha256	2c26b46b68ffc68ff99b453c1d30413413422d706483bfa0f98a5e886266e7ae				✓				Inherit	(0/0/0)		
2026-04-05		Network activity	domain	update-microsoft365.com				✓				Inherit	(0/0/0)		
2026-04-05		Network activity	ip-dst	185.157.233.45				✓				Inherit	(0/0/0)		

« previous | next » | view all

Discussion

« previous | next »

Date: 2026-04-05 02:24:43 Top | #7

Rayan111

threat Status Confirmed Malicious
Contained Yes
Final Decision Block

ryan1112015@gmail.com

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

Emotet Macro Malware Attack

ID	95
UUID	1ae415e6-420f-4bdf-8965-8cf7d5648792
Event	#1833: Emotet Macro Malware Attack
Distribution	Inherit event
Last update	2026-04-05 02:22:23

Edit | Split Screen | Markdown | Raw | Save | Menu | Help

The attack started with a phishing email containing a malicious Office document. When the user enabled macros, malware was downloaded and installed on the system. The malware established persistence and communicated with a command and control server. The attacker then exfiltrated credentials and system information from the infected machine.

Spread Method

ID	97
UUID	e223f7c0-2040-45cd-ac16-9841a0b9d2df
Event	#1833: Emotet Macro Malware Attack
Distribution	**Your organisation only**
Last update	2026-04-05 02:27:38

Edit | Split Screen | Markdown | Raw | Save | Menu | Help

The attack spreads through phishing emails containing malicious Office documents with macros that download malware from external servers.

Attack Stages

ID	96
UUID	58ce57eb-cf09-4747-8227-325f6b4a1ede
Event	#1833: Emotet Macro Malware Attack
Distribution	**Your organisation only**
Last update	2026-04-05 02:26:16

Edit | Split Screen | Markdown | Raw | Save | Menu | Help

1. Phishing email delivery
2. User opened malicious document
3. Macro execution
4. Malware installation
5. Persistence established
6. Command and control communication
7. Credential exfiltration

Impact

ID	98
UUID	5b992187-34c2-4b28-83c7-ec3af04c1895
Event	#1833: Emotet Macro Malware Attack
Distribution	**Your organisation only**
Last update	2026-04-05 02:28:02

Edit | Split Screen | Markdown | Raw | Save | Menu | Help

Credential theft, system compromise, data exfiltration, lateral movement, and potential ransomware deployment.