

ALTAY TAKIMI

TRYHACKME SOC SIMULATOR

Gürkan Parlak

01.03.2025

1-Alert

1000

Suspicious email from external domain.

Low

Phishing

Mar 2nd 2025 at 05:43

Awaiting action

Description:

A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.

datasource:

emails

timestamp:

03/02/2025 02:40:50.077

subject:

You've Won a Free Trip to Hat Wonderland - Click Here to Claim

sender:

boone@hatventuresworldwide.online

recipient:

miguel.odonnell@tryhatme.com

attachment:

None

content:

The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.

direction:

inbound

İlk alert degerlendirme sürecinde:

splunkenterprise

Apps

Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

New Search

Close

enter search here...

1 hour window

Q

Server error

281 of 281 events matched

No Event Sampling

Job

11

1

2

3

4

5

6

Next

Events (281)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 minute per column

Table

Format

50 Per Page

Prev

1

2

3

4

5

6

Next

Hide Fields

All Fields

SELECTED FIELDS

event.code 7

host 1

host.name 14

index 1

process.name 27

sender 55

source 1

sourcetype 1

timestamp 100+

INTERESTING FIELDS

attachment 3

content 1

datasource 3

direction 3

event.action 9

file.path 18

linecount 1

process.command_line 45

process.parent.pid 43

Time

host

host.name

index

process.name

source

timestamp

event.code

sourcetype

sender

02/03/2025 02:48:01.000

1010.84.254.8989

main

main

eventcollector

03/02/2025 02:47:14.077

..json

sophie.j@tryhatme.com

02/03/2025 02:47:47.000

1010.84.254.8989

win-3452

main

seth.exe

eventcollector

03/02/2025 02:47:11.077

1

..json

02/03/2025 02:47:18.000

1010.84.254.8989

main

OUTLOOK.EXE

eventcollector

03/02/2025 02:46:59.077

22

..json

02/03/2025 02:47:07.000

1010.84.254.8989

main

eventcollector

03/02/2025 02:46:17.077

..json

miguel.odonnell@tryhatme.com

02/03/2025 02:46:59.000

1010.84.254.8989

main

eventcollector

03/02/2025 02:46:54.077

..json

yani.zubair@tryhatme.com

02/03/2025 02:46:47.000

1010.84.254.8989

main

eventcollector

03/02/2025 02:46:19.077

..json

liam.espinosa@tryhatme.com

02/03/2025 02:46:41.000

1010.84.254.8989

main

eventcollector

03/02/2025 02:46:33.077

..json

roger.fedorov@tryhatme.com

02/03/2025 02:46:27.000

1010.84.254.8989

win-3459

main

TSTheme.exe

eventcollector

03/02/2025 02:46:07.077

1

..json

02/03/2025 02:46:25.077

1010.84.254.8989

main

eventcollector

03/02/2025 02:46:25.077

..json

safa.prince@tryhatme.com

Önce SIEM arayüzünü kendi filtrelemesi ile tekrar düzenledim.

02/03/2025 02:42:41.000

1010.84.254.8989

main

eventcollector

03/02/2025 02:40:50.077

..json

boone@hatventuresworldwide.online

["datasource":"emails","timestamp":"03/02/2025 02:40:50.077","subject":"You've Won a Free Trip to Hat Wonderland - Click Here to Claim","sender":"boone@hatventuresworldwide.online","recipient":"miguel.odonnell@tryhatme.com","attachment":"None","content":"The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.","direction":"inbound"]

Type

Field

Value

Actions

Selected

host

1010.84.254.8989

index

main

sender

boone@hatventuresworldwide.online

source

eventcollector

sourcetype

..json

timestamp

03/02/2025 02:40:50.077

Event

attachment

None

content

The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.

datasource

emails

direction

inbound

recipient

miguel.odonnell@tryhatme.com

subject

You've Won a Free Trip to Hat Wonderland - Click Here to Claim

Time

_time

2025-03-02T02:42:41.000-00:00

Default

linecount

1

punct

[{"start": "02/03/2025 02:42:41.000", "end": "02/03/2025 02:42:41.000"}]

splunk_server

ip-10-10-40-195

Daha sonra ilgili alertin log kaydini incelemeye aldım

Yüksek seviye bir TLD sahip olduğuna dair bir not bulunmakta. Bu sebeple phishing olduğunu düşündüm ve true positive olarak değerlendirdim.

Incident report

Incident classification

☒ True positive ☐ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

B I U A ▼ ≡ ≡ ▼

High level TLD and suspicious mail content

Does this alert require escalation?

☐ Yes ☒ No

Submit and close alert

Bu şekilde bir raporlama yaptım.

2-Alert

1001	Suspicious email from external domain.	Low	Phishing	Mar 2nd 2025 at 05:44	Awaiting action	
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	03/02/2025 02:41:50.077					
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping					
sender:	maximilian@chicmillinerydesigns.de					
recipient:	michelle.smith@tryhatme.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	inbound					

Burada da phishing olduğu bariz bir şekilde belli. Mail adresinden ve içerik bakımından ayrıca not kısmında yüksek seviye TLD bahsediliyor.

Incident report

Edit report

Incident classification

☒ True positive ☐ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

High level TLD and phishing content

Does this alert require escalation?

☐ Yes ☒ No

Bu şekilde raporlama yaptım

3-Alert

1003	Reply to suspicious email.	^	Low	Phishing	Mar 2nd 2025 at 05:47	Awaiting action	👤
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.						
datasource:	emails						
timestamp:	03/02/2025 02:45:16.077						
subject:	FWD: Convention Registration Now Open: Hat Trends and Insights						
sender:	support@tryhatme.com						
recipient:	warner@yahoo.com						
attachment:	None						
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.						
direction:	outbound						

Burada herhangi önemli bir durum gözüküyor.

Incident report

Incident classification

☐ True positive ☒ False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▼ ☰ ☷ ☹ ▼

No problem.

Submit and close alert

Bu şekilde raporlama yaptım.

4-Alert

1004	Suspicious Attachment found in email	^	Low	Phishing	Mar 2nd 2025 at 05:49	Awaiting action	👤
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.						
datasource:	emails						
timestamp:	03/02/2025 02:46:54.077						
subject:	Force update fix						
sender:	yani.zubair@tryhatme.com						
recipient:	michelle.smith@tryhatme.com						
attachment:	forceupdate.ps1						
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.						
direction:	internal						

Burada true positive olarak değerlendirdim. Ancak false positive durumu varmış.

Incident report

Edit report

Incident classification

☒ True positive ☐ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

High risk file sharing and suspicious powershell usage

Does this alert require escalation?

☒ Yes ☐ No

Save and close alert

5-Alert

1005	Reply to suspicious email.	Low	Phishing	Mar 2nd 2025 at 05:49	Awaiting action	
Description:		An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:		emails				
timestamp:		03/02/2025 02:47:14.077				
subject:		Shrinking Hat Sale: Tiny Hats for Extraordinary People				
sender:		sophie.j@tryhatme.com				
recipient:		eileen@gmail.com				
attachment:		None				
content:		The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:		outbound				

Burada herhangi bir problem yoktu.

Incident report

Incident classification

☐ True positive ☒ False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▼ ▢ ▢ ▢ ▼

no problem

Submit and close alert

Bu şekilde raporladım.

6-Alert

1006	Suspicious email from external domain.	Low	Phishing	Mar 2nd 2025 at 05:51	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	03/02/2025 02:49:11.077				
subject:	Hats Off to Savings: Discounted Vacation Packages Just for You!				
sender:	tim@chicmillinerydesigns.de				
recipient:	invoice@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

Phising olduğunu düşündüğüm bir gönderici bulunmakta. Phising olabilir.

Incident report

Incident classification

☒ True positive ☐ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

B I U A ↕ ↗ ↘ ↙ ↚

suspicious mail content

Does this alert require escalation?

☐ Yes ☒ No

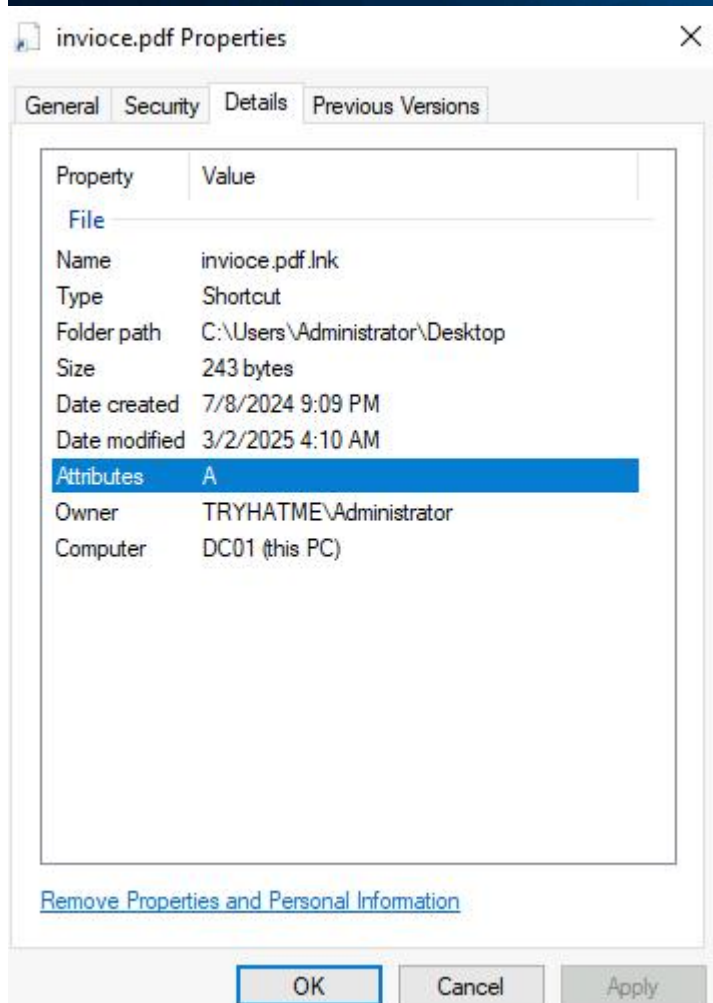
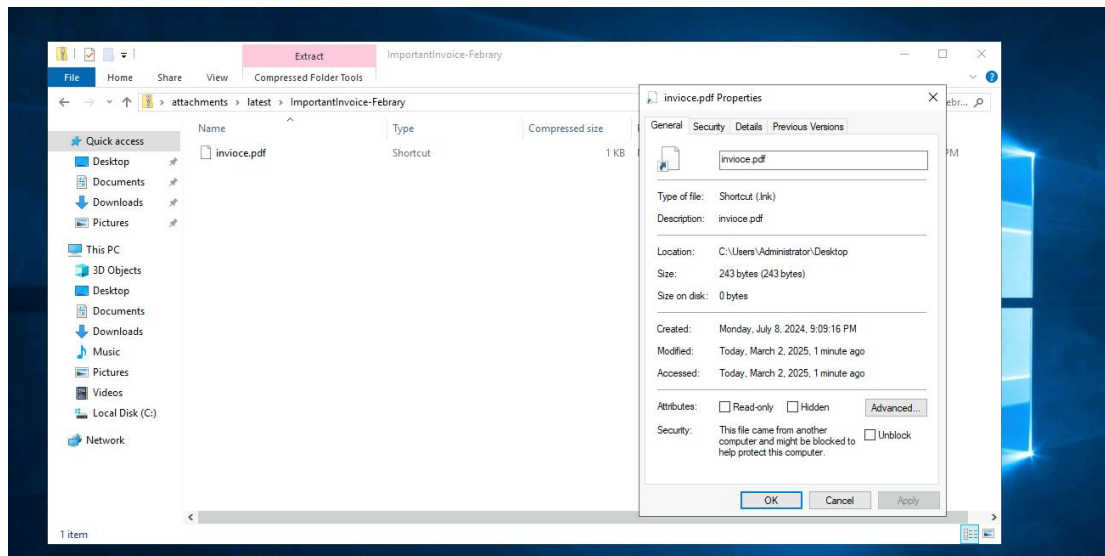
Submit and close alert

Bu şekilde raporladım.

7-Alert

Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.
datasource:	emails
timestamp:	03/02/2025 02:51:34.077
subject:	Important: Pending Invoice!
sender:	john@hatmakereurope.xyz
recipient:	michael.ascot@tryhatme.com
attachment:	ImportantInvoice-February.zip
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	inbound

Burada pdf uzantılı gözükken ancak pdf uzantısı olmayan bir dosya gönderilmiş. Son derece şüpheli ve yüksek riskli.



Incident report

Incident classification

☒ True positive☐ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

B I U A ▾

high level risk and suspicious file

Does this alert require escalation?

☒ Yes☐ No

Submit and close alert

Bu şekilde açıklama yaptım.

ID ▾	Alert rule ▾	Severity ▾	Type ▾	Time to resolve ▾	Classification ▾	Action
1000	Suspicious email from external domain.	Low	Phishing	2.1 minutes	✗ Incorrect	✎ View analysis
1001	Suspicious email from external domain.	Low	Phishing	1.98 minutes	✗ Incorrect	✎ View analysis
1004	Suspicious Attachment found in email	Low	Phishing	1.18 minutes	✗ Incorrect	✎ View analysis
1006	Suspicious email from external domain.	Low	Phishing	0.78 minutes	✗ Incorrect	✎ View analysis
1007	Suspicious Attachment found in email	Low	Phishing	0.72 minutes	✓ Correct	✎ View analysis

False positives

Assess your accuracy on the alerts you marked as false positives.

ID ▾	Alert rule ▾	Severity ▾	Type ▾	Time to resolve ▾	Classification ▾	Action
1003	Reply to suspicious email.	Low	Phishing	1.05 minutes	✓ Correct	🔗 View
1005	Reply to suspicious email.	Low	Phishing	0.38 minutes	✓ Correct	🔗 View

Sonuç tablosu.