



# **TryHackMe**

## **Introduction to Phishing**

**Hazırlayan:** Saliha Polat

**Tarih:** 01.03.2025

**A L T A Y**

**Olay Başlığı:** Şüpheli E-posta

**Alert Türü:** 1000 Suspicious email from external domain

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 14.28' da şüpheli e-posta davranışıyla ilgili SIEM üzerinden tespit edildi. Olay incelemesi sonucunda verilen domain adresine ait herhangi bir kötü amaçlı bulgu bulunmadı. False positive alarm olarak girildi.

## 2. Olay Açıklaması (Incident Description)

**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:** 02/28/2025 14:26:49.092

**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

## 3. Kapsam (Scope)

Etkilenen Kullanıcı: miguel.odonnell@tryhatme.com

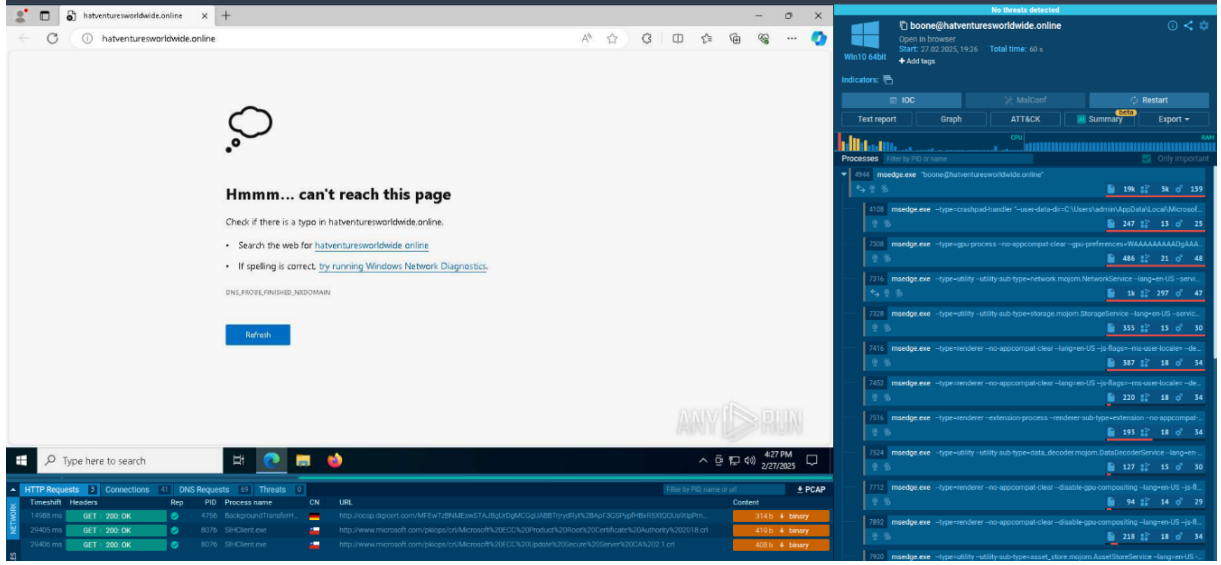
Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

Gönderen Kullanıcı: boone@hatventuresworldwide.online

## 4. İnceleme (Investigation)

Time	Event
28/02/2025 14:28:24.000	{ [-] 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 sender: boone@hatventuresworldwide.online subject: You've Won a Free Trip to Hat Wonderland - Click Here to Claim timestamp: 02/28/2025 14:26:28.839 } Show as raw text host = 10.10.222.184:8989   source = eventcollector   sourcetype = _json



## 5. Bulgular (Findings)

Hedef e-posta adresine şüpheli bir e-posta düşmüştür ve gerekli incelemeler yapıldıktan sonra bu alert False Positive olarak işaretlenmiştir.

## 6. Sonuç (Conclusion)

Zararlı işaretlenecek herhangi bir bulgu bulunamamıştır.

False positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM' de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (AnyRun, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
- AnyRun Taraması
- VirusTotal Taraması

**Olay Başlığı:** Şüpheli E-posta

**Alert Türü:** 1001 Suspicious email from external domain

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 14.28' de şüpheli e-posta davranışıyla ilgili SIEM üzerinden tespit edildi. Olay incelemesi sonucunda verilen domain adresine ait herhangi bir kötü amaçlı bulgu bulunmadı. False positive alarm olarak girildi.

## 2. Olay Açıklaması (Incident Description)

**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:** 02/28/2025 14:27:28.839

**subject:** VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping

**sender:** maximillian@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

## 3. Kapsam (Scope)

Etkilenen Kullanıcı: michelle.smith@tryhatme.com

Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

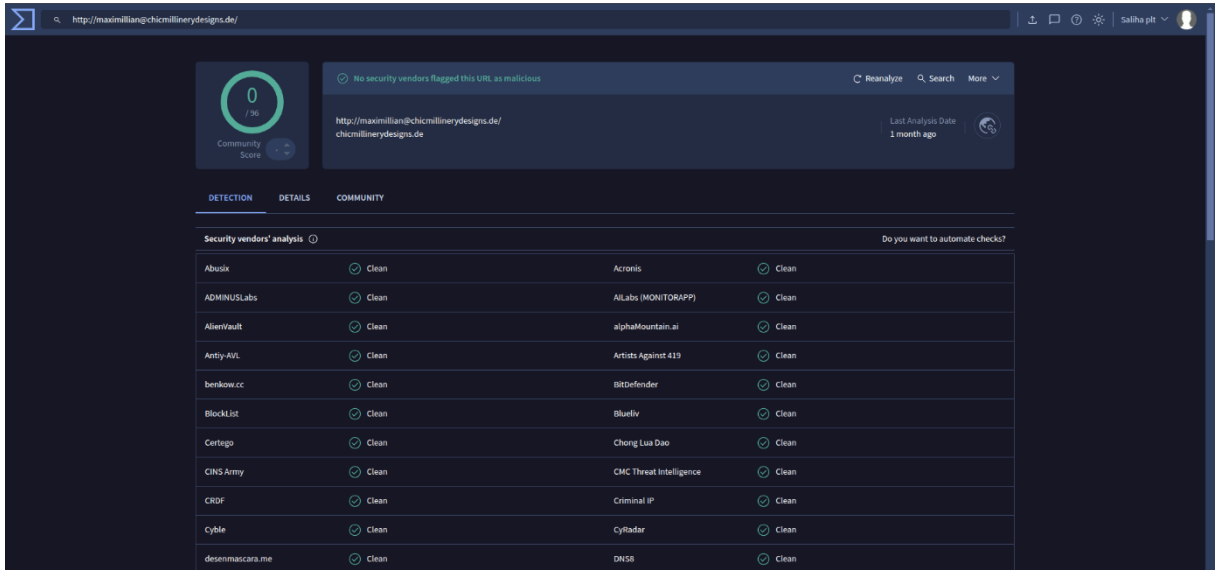
Gönderen Kullanıcı: maximillian@chicmillinerydesigns.de

## 4. İnceleme (Investigation)

Time	Event
28/02/2025 14:28:24.000	<pre>{ [-]   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: michelle.smith@tryhatme.com   sender: maximilian@chicmillinerydesigns.de   subject: VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping   timestamp: 02/28/2025 14:27:28.839 }</pre> <p>Show as raw text</p> <p>host = 10.10.222.184:8989   source = eventcollector   sourcetype = _json</p>

## 5. Bulgular (Findings)

Hedef e-posta adresine şüpheli bir e-posta düşmüştür ve gerekli incelemeler yapıldıktan sonra bu alert False Positive olarak işaretlenmiştir.



## 6. Sonuç (Conclusion)

Zararlı işaretlenecek herhangi bir bulgu bulunamamıştır.

False positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM' de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (AnyRun, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
- AnyRun Taraması
- VirusTotal Taraması

**Olay Başlığı:** Şüpheli parent-child işlemi

**Alert Türü:** 1002 Suspicious Parent Child Relationship

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 14.29' da olağan dışı bir parent-child işlemi tespit edildiği için SIEM üzerinden alert oluşmuştur. Olay incelemesi sonucunda herhangi bir kötü amaçlı bulgu bulunmadı. Bu işlemin olağan bir sistem aktivitesi olduğu tespit edildi. False positive alarm olarak girildi.

## 2. Olay Açıklaması (Incident Description)

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 02/28/2025 14:29:37.839

**event.code:** 1

**host.name:**

**process.name:** taskhostw.exe

**process.pid:** 3897

**process.parent.pid:** 3902

**process.parent.name:** svchost.exe

**process.command\_line:** taskhostw.exe NGCKKeyPregen

**process.working\_directory:** C:\Windows\system32\

**event.action:** Process Create (rule: ProcessCreate)

## 3. Kapsam (Scope)

Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

## 4. İnceleme (Investigation)

Format Timeline ▾ Zoom Out + Zoom to Selection X Deselect 1 minute per column

9 events at 16:58 Thursday, February 27, 2025

List ▾ Format 50 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a datasource 1
- a event.action 1
- # event.code 1
- a host.name 1
- a index 1
- # linecount 1
- a process.command\_line 2
- a process.name 1
- a process.parent.name 1
- # process.parent.pid 3
- # process.pid 3
- a process.working\_directory 1
- a punct 1
- a splunk\_server 1
- a timestamp 3

+ Extract New Fields

Time Event

27/02/2025 17:05:09.000

```
[...]  
datasource: sysmon  
event.action: Process Create (rule: ProcessCreate)  
event.code: 1  
host.name:  
process.command_line: taskhostw.exe NGCKeyPregen  
process.name: taskhostw.exe  
process.parent.name: svchost.exe  
process.parent.pid: 3880  
process.pid: 3649  
process.working_directory: C:\Windows\system32\  
timestamp: 02/27/2025 17:04:26.092  
]
```

Show as raw text

Type	Field	Value	Actions
Selected	host	10.10.250.1518989	▾
	source	eventcollector	▾
	sourcetype	_json	▾
Event	datasource	sysmon	▾
	event.action	Process Create (rule: ProcessCreate)	▾
	event.code	1	▾
	host.name		▾
	process.command_line	taskhostw.exe NGCKeyPregen	▾
	process.name	taskhostw.exe	▾
	process.parent.name	svchost.exe	▾
	process.parent.pid	3880	▾
	process.pid	3649	▾
	process.working_directory	C:\Windows\system32\	▾
	timestamp	02/27/2025 17:04:26.092	▾
Time	_time	2025-02-27T17:05:09.000+00:00	▾
Default	index	main	▾
	linecount	1	▾
	punct		▾
	splunk_server	ip-10-10-40-195	▾

1 \* "process.pid"=3897 1 hour window

Server error

1 of 1 event matched No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection X Deselect 1 minute per column

List ▾ Format 50 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a datasource 1
- a event.action 1
- # event.code 1
- a host.name 1
- a index 1
- # linecount 1
- a process.pid 1
- a punct 1
- a registry.key 1
- a registry.path 1
- a registry.value 1
- a splunk\_server 1
- a timestamp 1

+ Extract New Fields

Time Event

27/02/2025 16:50:51.000

```
[...]  
datasource: sysmon  
event.action: Registry value set (rule: RegistryEvent)  
event.code: 13  
host.name:  
process.pid: 3897  
registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-F452-47F9-826D-B41CFD35E447}\FriendlyName  
registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-F452-47F9-826D-B41CFD35E447}\FriendlyName  
registry.value: FriendlyName  
timestamp: 02/27/2025 16:50:26.892  
]
```

Show as raw text

Type	Field	Value	Actions
Selected	host	10.10.250.1518989	▾
	source	eventcollector	▾
	sourcetype	_json	▾
Event	datasource	sysmon	▾
	event.action	Registry value set (rule: RegistryEvent)	▾
	event.code	13	▾
	host.name		▾
	process.pid	3897	▾
	registry.key	System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-F452-47F9-826D-B41CFD35E447}\FriendlyName	▾
	registry.path	HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-F452-47F9-826D-B41CFD35E447}\FriendlyName	▾
	registry.value	FriendlyName	▾
	timestamp	02/27/2025 16:50:26.892	▾
Time	_time	2025-02-27T16:50:51.000+00:00	▾
Default	index	main	▾
	linecount	1	▾

### New Search

1 \* "process.pid"=3897  
2 | table process.name, process.parent.name, process.working\_directory

Server error

2 of 2 events matched No Event Sampling ▾

Events (2) Patterns Statistics (2) Visualization

100 Per Page ▾ Format

process.name	process.parent.name	process.working_directory
taskhostw.exe	svchost.exe	C:\Windows\system32\

## 5. Bulgular (Findings)

Yapılan incelemeler sonucunda belirtilen sonuçlar arasındaki ilişkinin normal olduğu görülmüştür.

## 6. Sonuç (Conclusion)

Zararlı işaretlenecek herhangi bir bulgu bulunmamıştır.

False positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM’ de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
- VirusTotal Taraması

---

**Olay Başlığı:** Şüpheli E-posta

**Alert Türü:** 1003 Reply to suspicious email.

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 14.31’ de şüpheli e-posta davranışıyla ilgili SIEM üzerinden tespit edildi. Olay incelemesi sonucunda verilen alan adlarına ait herhangi bir kötü amaçlı bulgu bulunmadı. False positive alarm olarak girildi.

## 2. Olay Açıklaması (Incident Description)

**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:** 02/28/2025 14:30:54.839

**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

### 3. Kapsam (Scope)

Etkilenen Kullanıcı: support@tryhatme.com

Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

Gönderen Kullanıcı: warner@yahoo.com

### 4. İnceleme (Investigation)

Time	Event
28/02/2025 14:31:33.000	<pre>{ [-]   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: outbound   recipient: warner@yahoo.com   sender: support@tryhatme.com   subject: FWD: Convention Registration Now Open: Hat Trends and Insights   timestamp: 02/28/2025 14:30:54.839 }</pre> <p>Show as raw text</p> <p>host = 10.10.222.184:8989   source = eventcollector   sourcetype = _json</p>

### 5. Bulgular (Findings)

Kaynaklardan alan adları tarandı ve herhangi kötü amaçlı bir bulguya rastlanmadı.

### 6. Sonuç (Conclusion)

Zararlı işaretlenecek herhangi bir bulgu bulunamamıştır.

False positive alert olarak işaretlenmiştir.

### 7. Aksiyonlar (Actions Taken)

- SIEM’ de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

### 8. Kaynakça (References)

- SIEM Log Kayıtları
  - VirusTotal Taraması
-

**Olay Başlığı:** Şüpheli E-posta Eki

**Alert Türü:** 1004 Suspicious Attachment found in email

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 14.32' de e-postayla gelen şüpheli ek bulunmasıyla ilgili SIEM'den alert oluşturuldu. Belirtilen dosyanın incelenmesinden sonra tehlike yaratacak herhangi bir unsur bulunmayıp alert False Positive olarak incelendi.

## 2. Olay Açıklaması (Incident Description)

**Description:** A suspicious attachment was found in the email. Investigate further to determine if it is malicious.

**datasource:** emails

**timestamp:** 02/28/2025 14:32:32.839

**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

## 3. Kapsam (Scope)

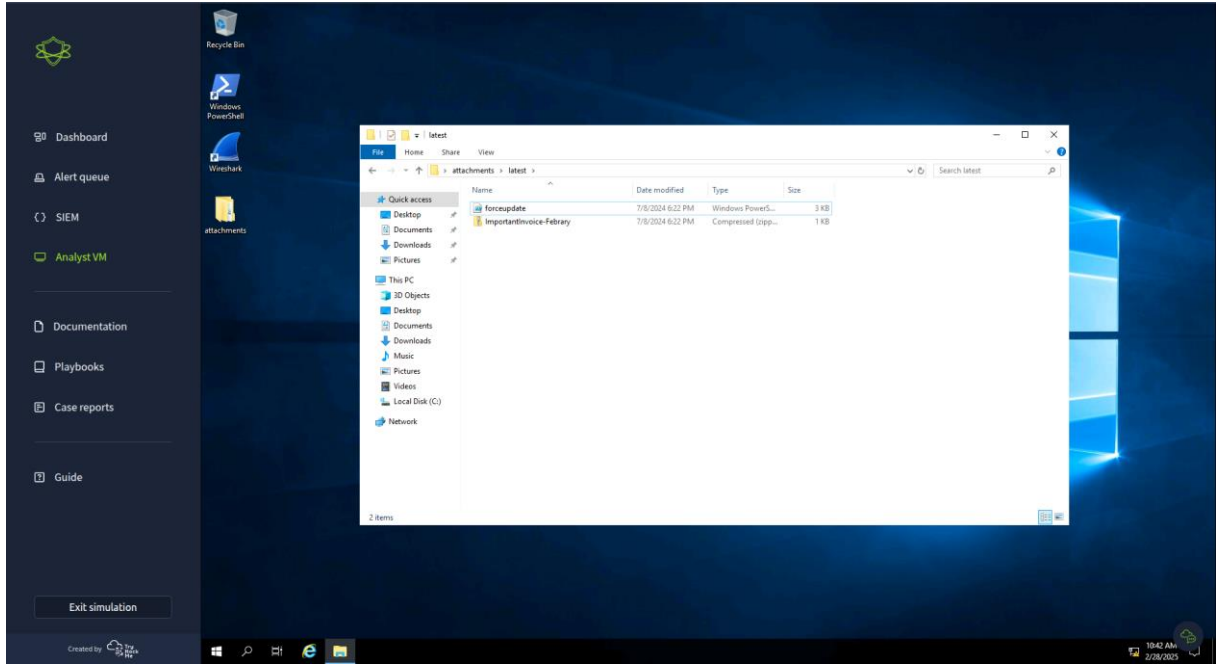
Etkilenen Kullanıcı: michelle.smith@tryhatme.com

Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

Gönderen Kullanıcı: yani.zubair@tryhatme.com

## 4. İnceleme (Investigation)



## 5. Bulgular (Findings)

Dosya incelendi ve herhangi bir zararlı bulguya rastlanmadı.

## 6. Sonuç (Conclusion)

Zararlı işaretlenecek herhangi bir bulgu bulunamamıştır.

False positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM’ de gelen alerte dair veriler incelendi.

- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, AnyRun, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
  - VirusTotal Taraması
  - AnyRun Taraması
- 

**Olay Başlığı:** Şüpheli E-posta

**Alert Türü:** 1005 Reply to suspicious email

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 17.33' de şüpheli e-posta davranışıyla ilgili SIEM üzerinden tespit edildi. Olay incelemesi sonucunda verilen alan adlarına ait herhangi bir kötü amaçlı bulgu bulunmadı. False positive alarm olarak girildi.

## 2. Olay Açıklaması (Incident Description)

**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:** 02/28/2025 14:32:52.839

**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

### 3. Kapsam (Scope)

Etkilenen Kullanıcı: eileen@gmail.com

Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

Gönderen Kullanıcı: sophie.j@tryhatme.com

### 4. İnceleme (Investigation)

Time	Event
28/02/2025 14:33:40.000	<pre>{ [-]   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: outbound   recipient: eileen@gmail.com   sender: sophie.j@tryhatme.com   subject: Shrinking Hat Sale: Tiny Hats for Extraordinary People   timestamp: 02/28/2025 14:32:52.839 }</pre> <p>Show as raw text</p> <p>host = 10.10.222.184:8989   source = eventcollector   sourcetype = _json</p>

### 5. Bulgular (Findings)

Hedef e-posta adresine şüpheli bir e-posta düşmüştür ve gerekli incelemeler yapıldıktan sonra bu alert False Positive olarak işaretlenmiştir

### 6. Sonuç (Conclusion)

Alan adları güvenilir, herhangi bir ek bulunmuyor.

Zararlı işaretlenecek herhangi bir bulgu bulunamamıştır.

False positive alert olarak işaretlenmiştir.

### 7. Aksiyonlar (Actions Taken)

- SIEM' de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, AnyRun, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

### 8. Kaynakça (References)

- SIEM Log Kayıtları
  - VirusTotal Taraması
  - AnyRun Taraması
-

**Olay Başlığı:** Şüpheli E-posta

**Alert Türü:** 1006 Suspicious email from external domain

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

## 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 17.35' de e-postayla gelen şüpheli ek bulunmasıyla ilgili SIEM'den alert oluşturuldu. Belirtilen dosyanın incelenmesinden sonra tehlike yaratacak herhangi bir unsur bulunmayıp alert False Positive olarak incelendi.

## 2. Olay Açıklaması (Incident Description)

**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:** 02/28/2025 14:34:49.839

**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

## 3. Kapsam (Scope)

Etkilenen Kullanıcı: fatura@tryhatme.com

Etkilenen Sistemler: Yok

Potansiyel Veri Sızıntısı: Yok

Gönderen Kullanıcı: tim@chicmillinerydesigns.de

## 4. İnceleme (Investigation)

Time	Event
28/02/2025 14:35:00.000	<pre>{ [-]   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: invoice@tryhatme.com   sender: tim@chicmillinerydesigns.de   subject: Hats Off to Savings: Discounted Vacation Packages Just for You!   timestamp: 02/28/2025 14:34:49.839 }</pre> <p>Show as raw text</p> <p>host = 10.10.222.184:8989   source = eventcollector   sourcetype = _json</p>

## 5. Bulgular (Findings)

Hedef e-posta adresine şüpheli bir e-posta düşmüştür ve gerekli incelemeler yapıldıktan sonra bu alert False Positive olarak işaretlenmiştir

## 6. Sonuç (Conclusion)

Alan adları güvenilir, herhangi bir ek bulunmuyor.

Zararlı işaretlenecek herhangi bir bulgu bulunamamıştır.

False positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM' de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, AnyRun, VirusTotal vb.)
- Alert false positive olarak işaretlenerek kapatıldı.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
  - VirusTotal Taraması
  - AnyRun Taraması
-

**Olay Başlığı:** Şüpheli E-posta

**Alert Türü:** 1007 Suspicious Attachment found in email

**Rapor Tarihi:** 28/02/2025

**Hassasiyet Seviyesi:** Düşük

**Analist:** Saliha Polat

### 1. Özet (Summary)

28 Şubat 2025 tarihinde saat 17.39' de e-postayla gelen şüpheli ek bulunmasıyla ilgili SIEM'den alert oluşturuldu. Belirtilen dosyanın incelenmesinden sonra zararlı davranışlar tespit edildi. Alert True Positive olarak işaretlendi.

### 2. Olay Açıklaması (Incident Description)

**Description:** A suspicious attachment was found in the email. Investigate further to determine if it is malicious.

**datasource:** emails

**timestamp:** 02/28/2025 14:37:12.839

**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

### 3. Kapsam (Scope)

Etkilenen Kullanıcı: michael.ascot@tryhatme.com

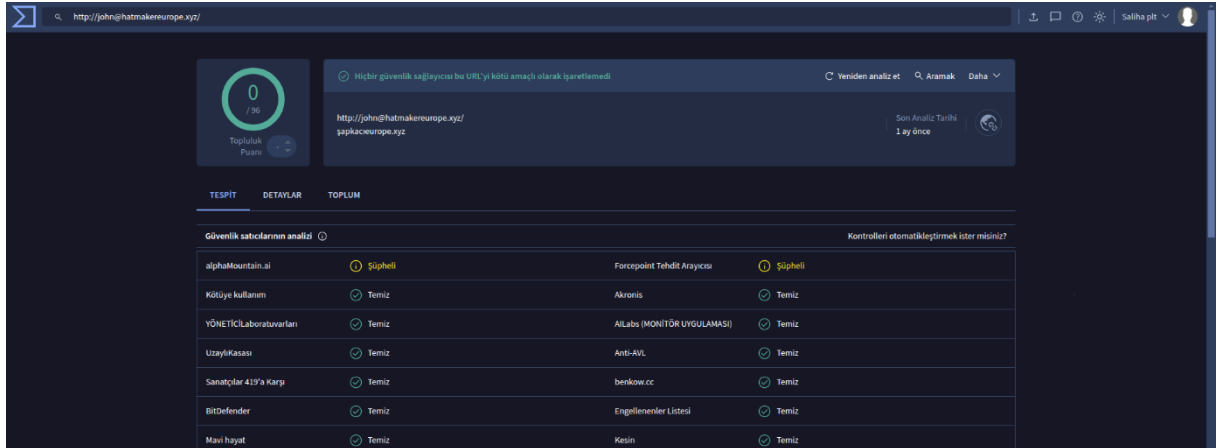
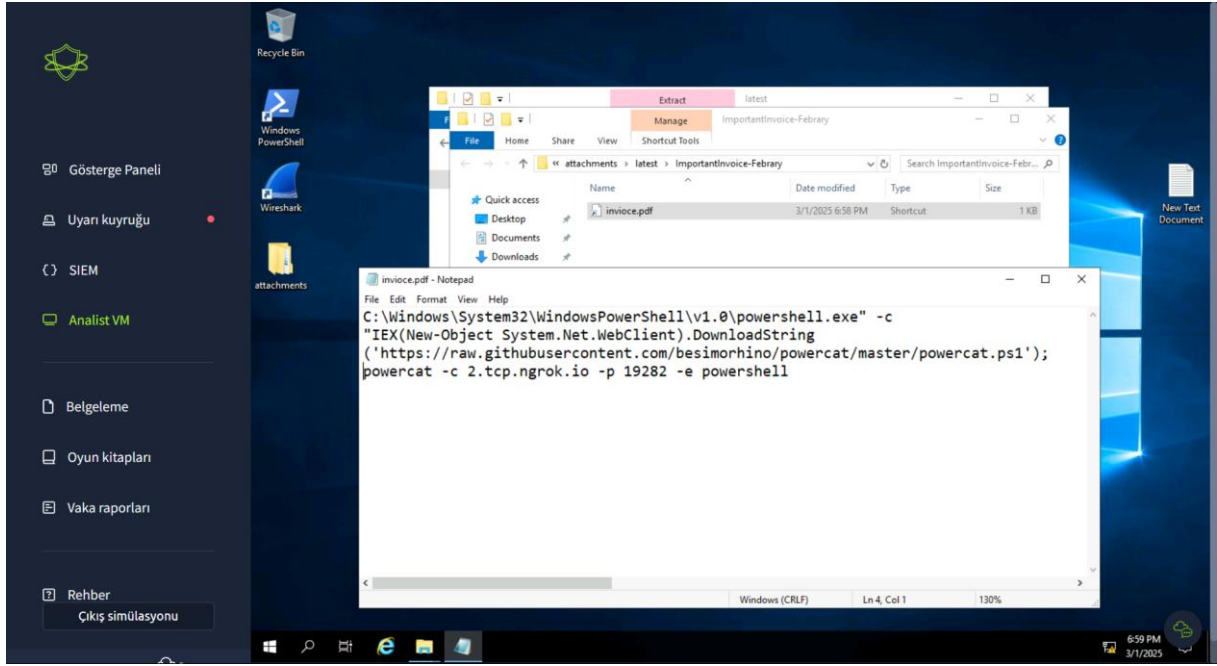
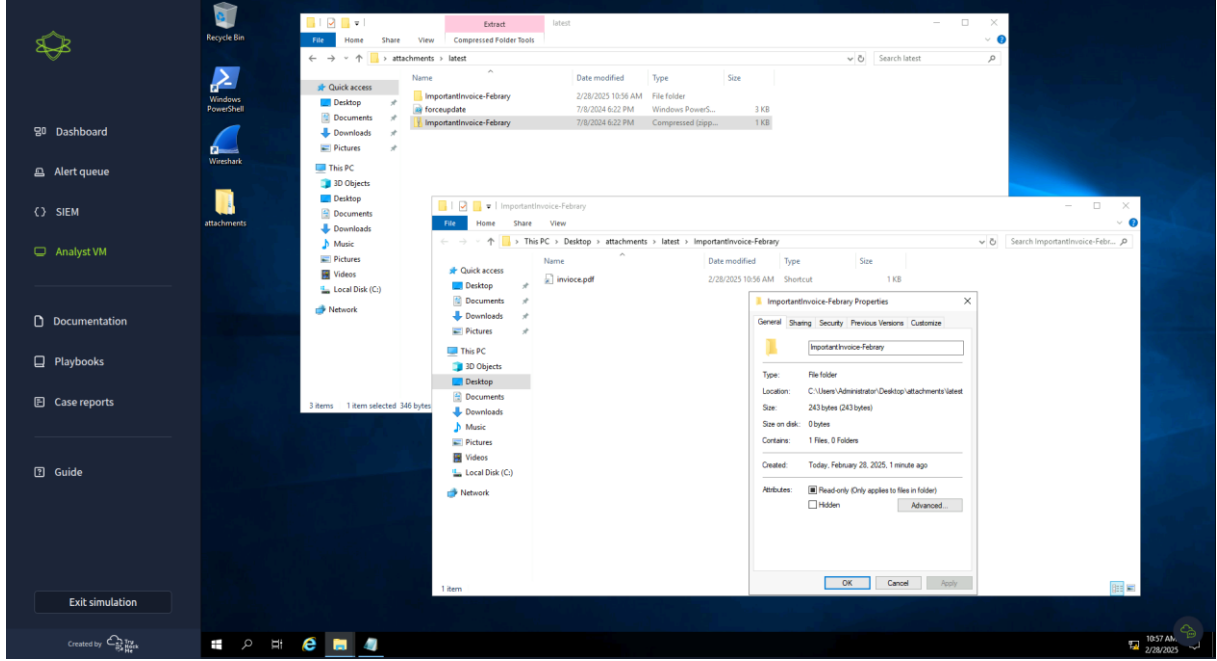
Etkilenen Sistemler: Yok

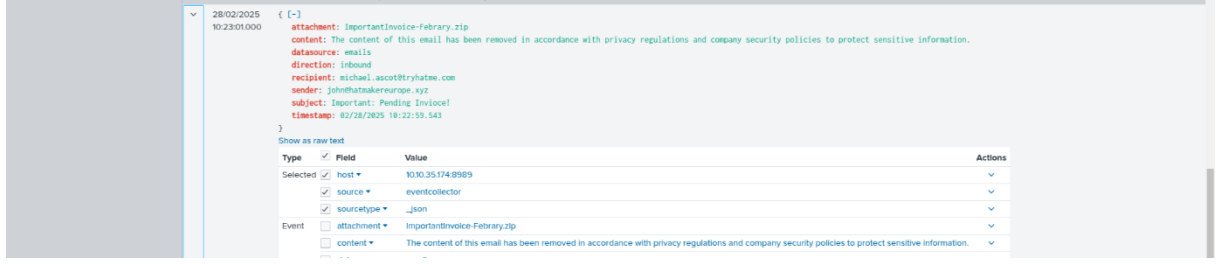
Potansiyel Veri Sızıntısı: Yok

Gönderen Kullanıcı: john@hatmakereurope.xyz



## 4. İnceleme (Investigation)





## 5. Bulgular (Findings)

Dosya incelendi “Important: Pending Invoice!” ibaresi kullanılarak gönderilen ImportantInvoice-February.zip adındaki zip dosyasının hedef sistemde PowerShell üzerinden PowerCat.ps1 aracının çalıştırıldığı tespit edilmiştir.

## 6. Sonuç (Conclusion)

Tespit edilen aktivite, saldırganın hedef sisteme erişim sağlamak amacıyla reverse shell bağlantısı kurmaya çalıştığını göstermektedir.

Bu olay kritik seviyede değerlendirilmiştir ve sistemin güvenliği sağlanana kadar gerekli izolasyon ve inceleme işlemleri devam ettirilmelidir.

True positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM’ de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, AnyRun, VirusTotal vb.)
- Alert true positive olarak işaretlenerek kapatıldı.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
- VirusTotal Taraması
- AnyRun Taraması

## Genel Sonuç (Overall Conclusion)

28 Şubat 2025 tarihinde SIEM üzerinden oluşturulan **7 farklı alarm** detaylı olarak incelenmiştir. Yapılan analizler sonucunda:

- **6 alarmın false positive** olduğu tespit edilmiş, herhangi bir kötü amaçlı aktiviteye rastlanmamıştır. Bu alarmlar ilgili kaynaklardan (SIEM, VirusTotal, AnyRun, Splunk vb.) doğrulama yapılarak kapatılmıştır.
- **1 alarm true positive** olarak değerlendirilmiş olup, ilgili dosya analizi sonucunda **PowerCat.ps1 aracı üzerinden reverse shell bağlantısı kurulmaya çalışıldığı** tespit edilmiştir. Gerekli izolasyon ve önlem süreçleri başlatılmıştır.

Tüm olaylar kayıt altına alınmış ve güvenlik kontrolleri tamamlanmıştır.