

Introduction to Phishing

Hazırlayan: Sinan Kocagöz

Tarih: 28.02.2025



İçindekiler Tablosu

1. Giriş	3
2. Kapsam ve Yöntem	4
3. Kullanılan Araçlar.....	4
4. Analiz Süreci	4
5. Bulgular	4
6. Sonuç.....	8



1. Giriş

Bu çalışmanın temel amacı, gerçek zamanlı phishing (oltalama) alarmlarını analiz etmek ve belirli bir zaman dilimi içinde bu alarmları doğru bir şekilde değerlendirmektir. Bu çalışmada:

- Gerçek zamanlı phishing girişimlerini tespit etmek ve analiz etmek.
- Gelen alarmların true positive (doğru pozitif) veya false positive (yanlış pozitif) olup olmadığını ayırt etmek.
- Log verilerini inceleyerek alarm kaynağını ve nedenini belirlemek.



2. Kapsam ve Yöntem

Bu simülasyon çalışması, 15 dakikalık bir zaman diliminde gerçekleştirilmiştir. Çalışma süresince aşağıdaki adımlar izlenmiştir:

- Splunk SIEM panelinde gelen alarmlar incelendi.
- Alarmların kaynağı ve ilgili log verileri detaylı bir şekilde analiz edildi.
- Elde edilen bulgulara göre alarmin true positive (gerçek tehdit) veya false positive (yanlış alarm) olduğu belirlen

3. Kullanılan Araçlar

Splunk: Gerçek zamanlı alarm izleme ve log analizi için kullanılan SIEM aracı.

TryHackMe: SOC simülasyon ortamını sağlayan platformu.

4. Analiz Süreci

Alarmların kaynağına ait log verileri incelendi.

Ağ trafiği ve sistem kayıtları üzerinde anormallikler araştırıldı.

Şüpheli aktiviteler belirlenerek olası phishing girişimleri analiz edildi.

5. Bulgular

Alarm 1000: Suspicious email from external domain

1000	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 17:12	
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:	03/01/2025 14:09:43.940				
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				

Severity: Low

Type: Phishing

Time to Resolve: 1.07 dakika

Sınıflandırma: False Positive, Harici bir alan adından gelen e-posta, ilk bakışta şüpheli görünse de yapılan analizde herhangi bir zararlı içerik veya kötü niyetli bağlantı tespit edilmemiştir. Bu nedenle alarm yanlış pozitif olarak değerlendirilmiştir.

Alarm 1001: Suspicious email from external domain

1001	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 17:13	
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:	03/01/2025 14:10:43.940				
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				

Severity: Low

Type: Phishing

Time to Resolve: 0.92 dakika

Sınıflandırma: False Positive, E-postanın geldiği alan adı incelenmiş ve güvenilir bir kaynağa ait olduğu doğrulanmıştır. İçerikte herhangi bir phishing göstergesi tespit edilmemiştir.

Alarm 1002: Suspicious Parent Child Relationship

1002	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 17:15	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 14:12:52.940				
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 NGCKeyPregen				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Time to Resolve: 0.58 dakika

Sınıflandırma: False Positive Bir işlem ilişkisine dayalı bu alarm, güvenlik politikalarına uygun bir sistem sürecinden kaynaklanmıştır. Bu nedenle yanlış pozitif olarak değerlendirilmiştir.

Alarm 1003: Reply to Suspicious Email

1003	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 17:16	👤-
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:	03/01/2025 14:14:09.940					
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					

Severity: Low

Type: Phishing

Time to Resolve: 0.62 dakika

Sınıflandırma: False Positive, Bu alarm, bir kullanıcının şüpheli olarak işaretlenmiş bir e-postaya yanıt verdiğini göstermektedir. Yapılan analiz sonucunda, orijinal e-postanın güvenli olduğu belirlenmiştir, dolayısıyla bu alarm yanlış pozitif olarak sınıflandırılmıştır.

Alarm 1004: Suspicious Attachment Found in Email

1004	Suspicious Attachment found in email	^	Low	Phishing	Mar 1st 2025 at 17:18	👤-
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	03/01/2025 14:15:47.940					
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					

Severity: Low

Type: Phishing

Time to Resolve: 0.98 dakika

Sınıflandırma: False Positive, E-postaya eklenmiş dosya analiz edilmiş ve herhangi bir zararlı yazılım belirtisine rastlanmamıştır. Dosyanın meşru bir iş iletişiminin parçası olduğu anlaşılmıştır.

Alarm 1005: Reply to Suspicious Email

1005	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 17:18	👤-
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:	03/01/2025 14:16:07.940					
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					

Severity: Low

Type: Phishing

Time to Resolve: 0.58 dakika

Sınıflandırma: False Positive, Kullanıcının yanıt verdiği e-posta incelenmiş ve güvenilir bir kaynaktan geldiği anlaşılmıştır. Phishing göstergesi bulunmamaktadır.

Alarm 1006: Suspicious Email from External Domain

1006	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 17:20	👤-
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:	03/01/2025 14:18:04.940					
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					

Severity: Low

Type: Phishing

Time to Resolve: 0.47 dakika

Sınıflandırma: False Positive, E-posta, dış bir kaynaktan gelmiş olmasına rağmen yapılan analiz sonucunda herhangi bir tehdit unsuru taşımadığı belirlenmiştir.

Alarm 1007: Suspicious Attachment Found in Email

1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 17:22	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:	emails				
timestamp:	03/01/2025 14:20:27.940				
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				

Severity: Low

Type: Phishing

Time to Resolve: 0.8 dakika

Sınıflandırma: True Positive, Bu alarmda, bir e-postaya eklenmiş şüpheli bir dosya tespit edilmiştir. Dosya, bilinen zararlı yazılım göstergelerine sahip olduğundan ve daha önce kara listeye alınmış bir kaynaktan geldiği için alarm doğru pozitif olarak sınıflandırılmıştır.

6. Sonuç

SOC simülasyonu, gerçek zamanlı phishing alarm analizine yönelik pratik kazandırdı ve Splunk aracı ile etkin bir şekilde güvenlik izleme yapılmasına katkı sağladı. True positive ve false positive alarmların ayırt edilmesi ve bu sınıflandırmanın log verileri ile desteklenmesi sayesinde, bir SOC analistinin sahip olması gereken araştırma ve analiz becerileri geliştirmiş oldum.