Phishing Unfolding

İREM GÜZEL
01.03.2025

İçindekiler Tablosu

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

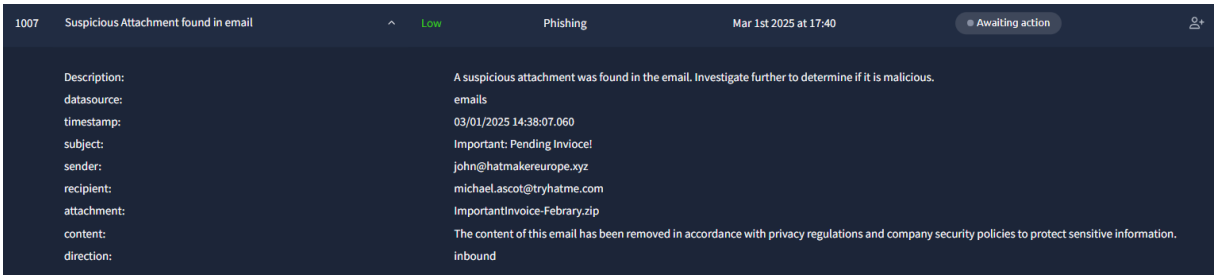
Miguel O'Donnell, Sales miguel.odonnell@tryhatme.com Logged-in host: win-3451

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



Sender : john@hatmakereurope.xyz

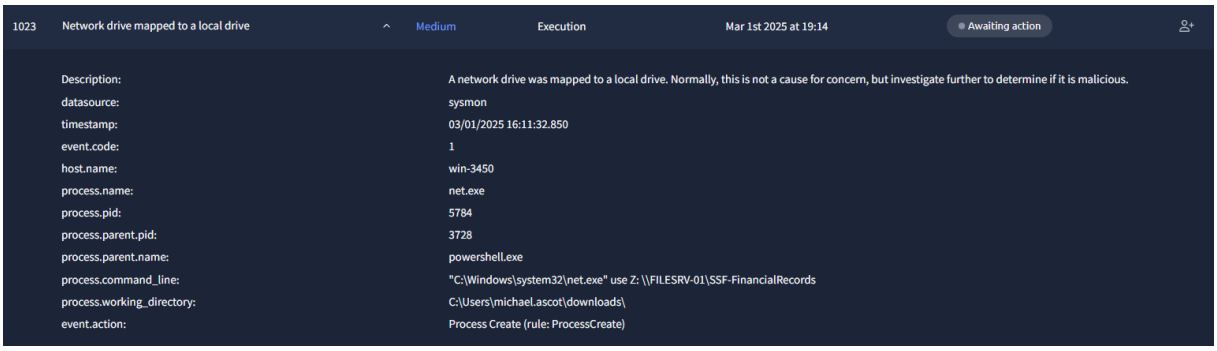
Domain : hatmakereurope.xyz

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

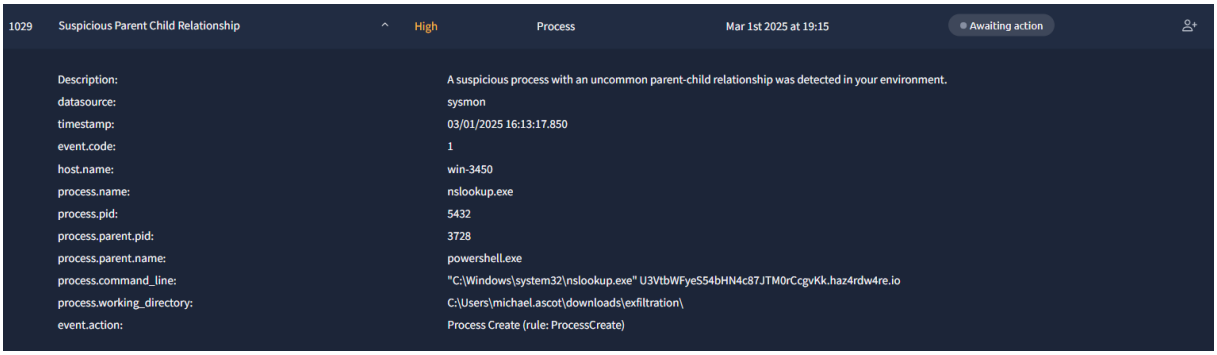


process.parent.name: powershell.exe

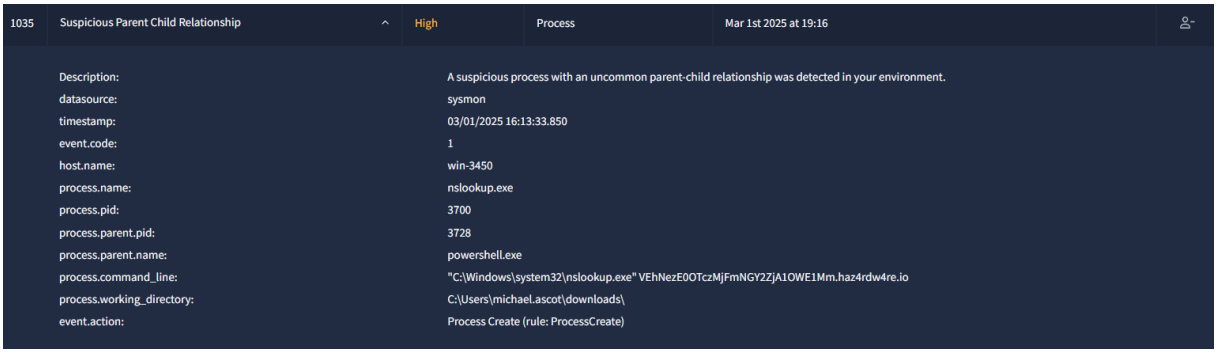
Powershell ile Z sürücüsüne ağ bağlantısı açılmış.Bu ağdan da SSF-FinancialRecords büyük ihtimalle finansal kayıtların olabileceği dosyanın paylaşımı yapılmış.

ID 1027

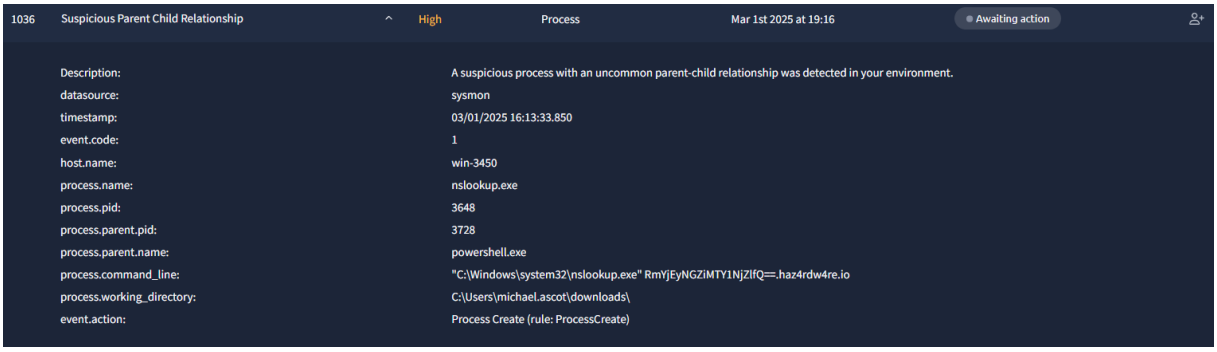
ID 1029



ID 1035



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



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