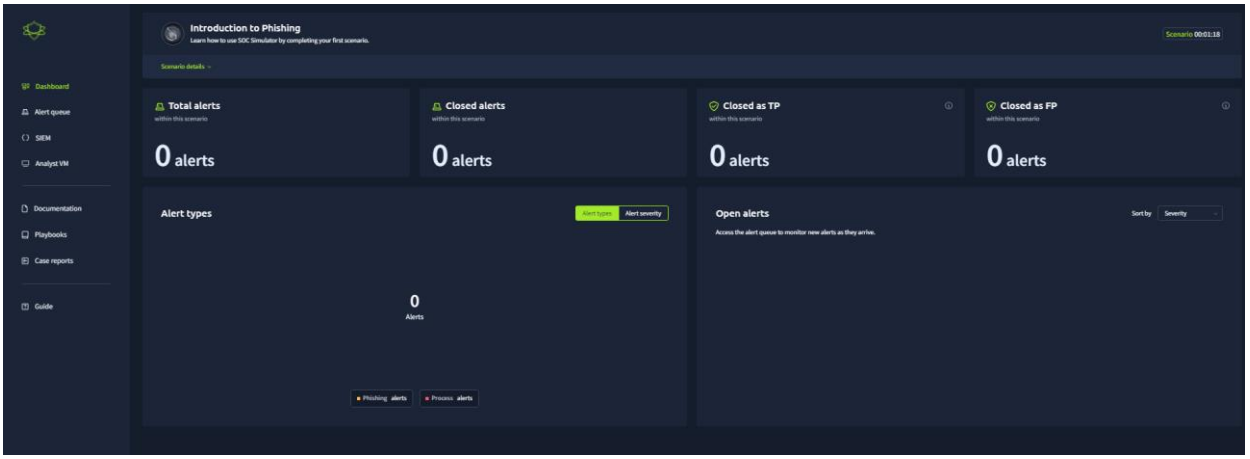
Introduction Phishing Write-Up

Hazırlayan: Esra Akteke

Tarih: 01.03.2025

Arayüz İncelemesi

İlk giriş yaptığımızda aşağıdaki gibi bir ekran ile karşılaşıyoruz. Arayüzü incelediğimizde, sol bölümde Dashboard, Alert queue, SIEM, Analyst VM, Documention, Playbooks, Case reports, Guide seçeneklerini görmekteyiz. Bu bölümlerin ne olduğunu kısaca anlatmak gerekirse;



Dashboard: Genel güvenlik durumunu, aktif tehditleri ve kritik olayları özetleyen ana kontrol panelidir.

Alert Queue: Tespit edilen güvenlik olaylarının sıralandığı ve SOC analistleri tarafından incelenmeyi bekleyen uyarıların bulunduğu bölümdür.

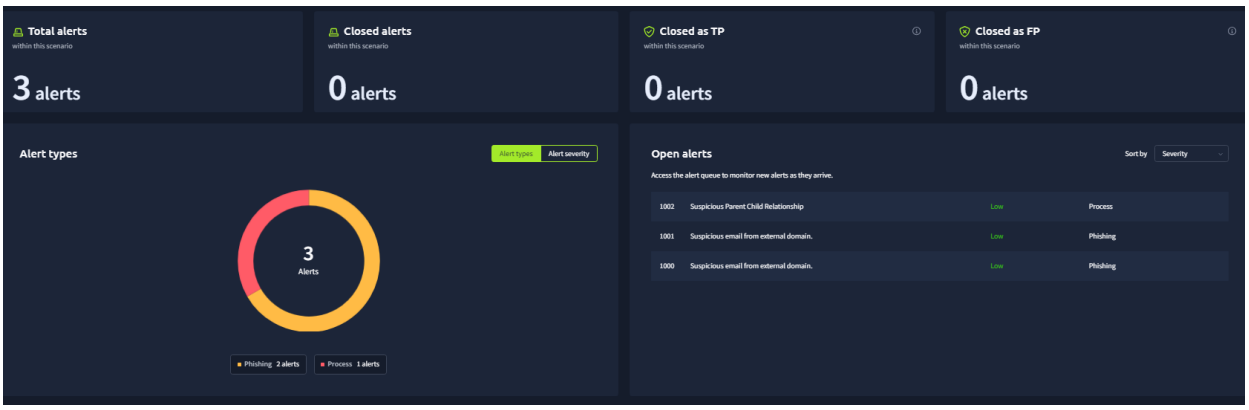
SIEM: Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemine erişim sağlar. Bu bölümde loglar toplanır, analiz edilir ve korelasyon kuralları ile tehdit tespiti yapılır.

Analyst VM: Analistlerin zararlı dosyaları inceleyebileceği, güvenli bir test ortamı sunan sanal makine bölümüdür.

Documentation: SOC süreçleri, olay müdahale prosedürleri ve sistemlerin nasıl çalıştığına dair dokümantasyonların yer aldığı bölümdür.

Playbooks: Farklı saldırı senaryolarına karşı izlenmesi gereken adımları içeren otomatik veya manuel olay müdahale kılavuzlarıdır.

Case Reports: Geçmişte analiz edilen olayların raporlandığı, alınan aksiyonların ve sonuçların kaydedildiği bölümdür. Guide: SOC sistemine dair temel kullanım kılavuzlarını ve yeni analistlerin süreçleri öğrenmesine yardımcı olan belgeleri içeren bölümdür.

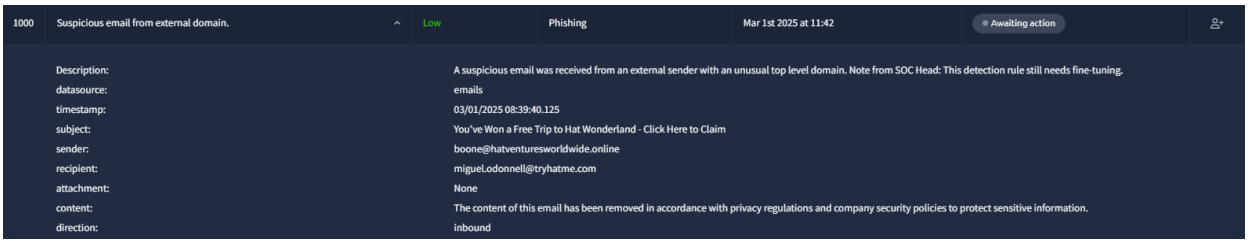


Arayüzü biraz daha incelediğimizde toplam gelen alarm sayısını, kapatılmış alarmları vb. bilgisini alabildiğimizi görüyoruz.

Şimdi Alert queue kısmına girerek gelen alarmları sırasıyla analiz edip ticketları kapatalım.

Alarm Bilgisi ID:1000

1000 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.



Kuruluşa ait güvenlik sistemleri tarafından alışılmadık bir üst düzey etki alanına sahip harici bir göndericiden gelen şüpheli bir e-posta tespit edildiğini görmekteyiz. E-posta, "You've Won a Free Trip to Hat Wonderland - Click Here to Claim" konulu bir mesaj içeriyordu ve gönderici, Hatventures Worldwide'dan Boone olarak görünüyor.

Bu e-posta, **hatventuresworldwide.online** alan adını kullanarak Miguel O'Donnell'e gönderilmiş olup, harici bir kaynaktan içeriye doğru yönlendirilmiştir.

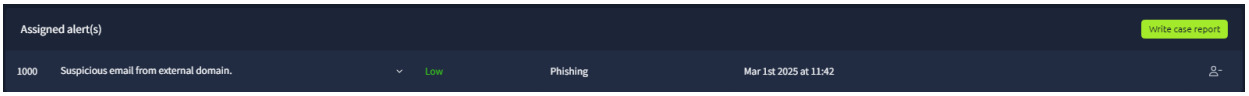
SOC Başkanı tarafından yapılan değerlendirmeye göre, bu tespit kuralının ince bir ayara ihtiyacı olabilir veya hâlâ geliştirilmesi gerekmektedir. Bu bilgiye ise description bölümünden ulaştığımızı söyleyebiliriz. Bu da, e-postanın yanlış pozitif olma ihtimalini düşündürmektedir.

Olayın tam zaman bilgisi, 03/01/2025 08:39:40.125 zaman damgası (timestamp) ile kaydedilmiştir.

Ayrıca, e-postanın içeriği gizlilik düzenlemeleri ve güvenlik politikaları gereği kaldırılmış olup, herhangi bir ek içermediği tespit edilmiştir.

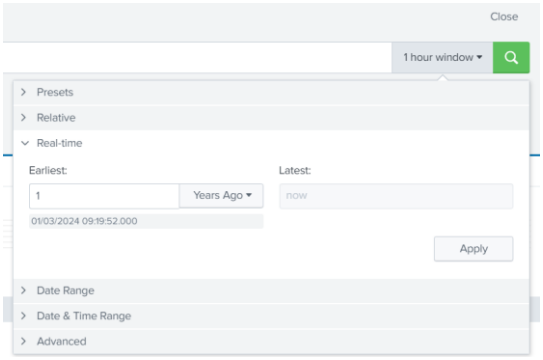
Alarm İncelemesi ID:1000

Öncelikle incelemeye başlamak adına Awaiting Action statüsünde bulunan1000 numaralı ID ye sahip olan alarmın sahipliğini üstleniyoruz. Üstlendiğimiz alarmların takibini buradan sağlayabilirsiniz. Assigned alerts bölümü üstümüze atanmış tüm alarmların toplandığı bölümdür.

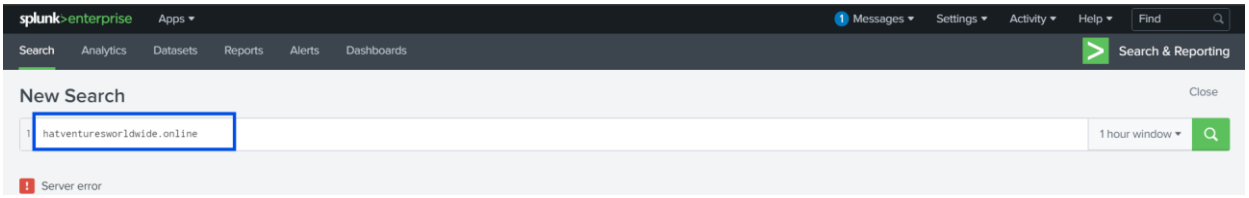


Olayı daha derinlemesine araştırmak için elimizdeki araçları etkili bir şekilde kullanmamız gerekiyor. Öncelikle Splunk üzerinden araştırmaya başlayarak, şüpheli e-posta ile ilişkili tehdit göstergelerini inceleyebiliriz.

İlk olarak, tüm ilgili olayları kapsayabilmek adına Splunk'taki zaman aralığını son 1 yılı kapsayacak şekilde ayarlıyoruz.

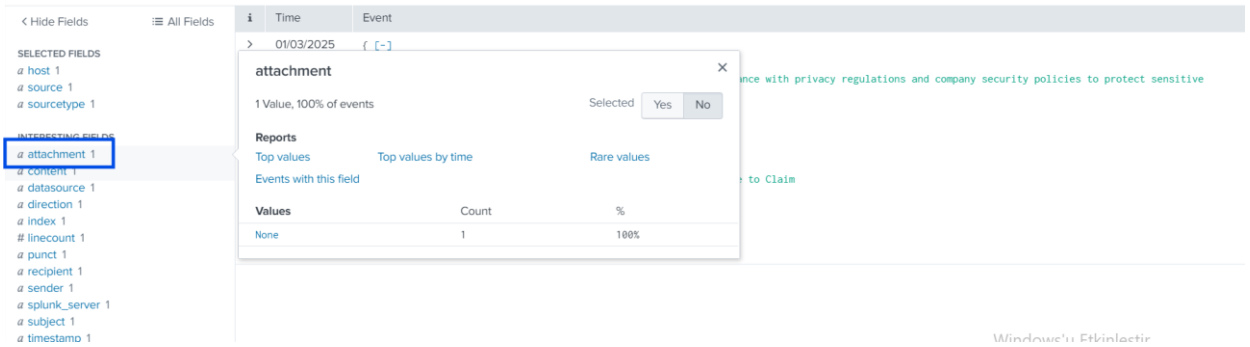


Bir sonraki aşamamızda Search kısmına, e-postada geçen şüpheli alan adını (hatventuresworldwide.online) girerek bu alan adının daha önce sistemde herhangi bir olayda geçip geçmediğini kontrol ediyoruz. Burada ki asıl amaç, çıkan olayları detaylı bir şekilde inceleyerek, bu alan adının geçmişte hangi olaylarla ilişkilendirildiğini belirlemeye çalışmak diyebiliriz.



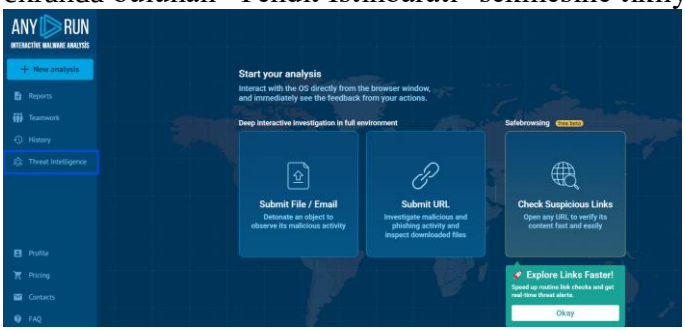
Burada görmüş olduğumuz Event daha önce gördüğümüz e-posta ile aynıdır.

Buradaki önemli nokta attachment kısmıdır. Bu alan, aslında bir ek olup olmadığını kontrol etmemizi sağlar. Value kısmını incelediğimizde "None" ifadesiyle karşılaşıyoruz. Görüldüğü üzere bu da herhangi bir ek bulunmadığını gösteriyor.



E-postanın içeriği güvenlik politikaları gereği kaldırıldığı için elimizde yalnızca alan adı bulunuyor. Herhangi bir ek dosya olmadığından, zararlı yazılım analizi yapmamıza gerek yok. Ancak alan adının güvenilirliğini ve potansiyel tehdit olup olmadığını anlamak için AnyRun ve VirusTotal gibi araçlarla daha derinlemesine analiz yaparak, şüpheli alan adının gerçekten kötü amaçlı olup olmadığını belirleyebiliriz.

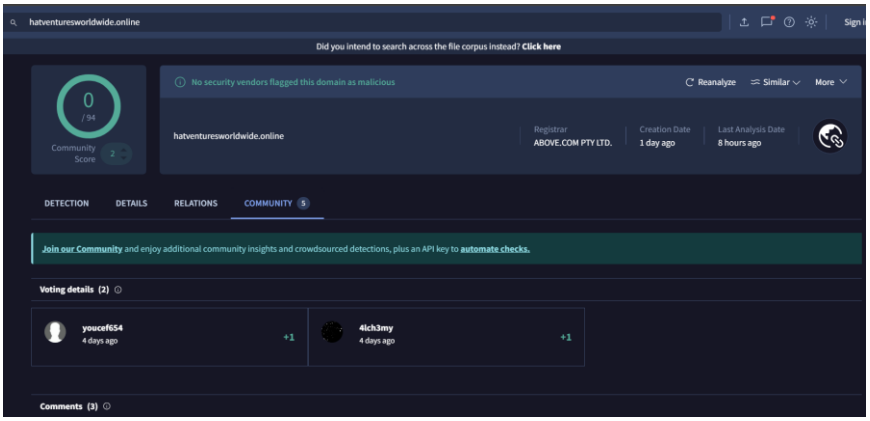
Öncelikle AnyRun üzerinden sorgulatma sağlıyoruz. Hesabınıza giriş yaptıktan sonra ana ekranda bulunan "Tehdit İstihbaratı" sekmesine tıklıyoruz.



Tehdit İstihbaratı" bölümüne, e-posta içeriğinden elde ettiğimiz hatventuresworldwide.online alan adını yapıştırıyoruz.

AnyRun bu alan adını daha önce kullanan kişilerin yaptığı analizleri gösteriyor. Eğer sonuçlar bu alan adıyla ilgili kötü amaçlı bir etkinlik olmadığını gösteriyorsa, bu alan adı hakkında endişelenmemize gerek olmadığını anlayabiliriz. Sonuçlar üzerinde kontrol sağladığımızda bu alan adını daha önce inceleyen diğer kullanıcıların analizlerine erişmemizi sağladı. Bu analizler, alan adının kötü amaçlı bir tehdit içermediğini ve zararlı faaliyetlerle ilişkilendirilmediğini gösterdi.

VirusTotal sitesine giriş yapıyoruz. Yine hatventuresworldwide.online alan adını aynı şekilde VirusTotal arama kutusuna yapıştırıyoruz. VirusTotal, alan adının kötü amaçlı olup olmadığını kontrol eder ve yapılan taramalarda kötü amaçlı bir işaret yoksa bu da alan adının güvenli olduğu anlamına gelir. Eğer VirusTotal'da da kötü amaçlı hiçbir etki görülmezse, bu sonuç da AnyRun ile elde ettiğimiz sonuçla uyumludur.

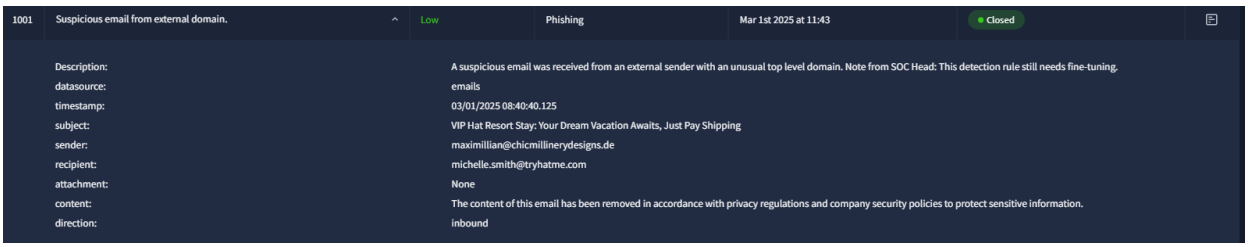


Kontrol sağladığımızda güvenli görünmektedir, aynı zamanda Community sekmesinden ise daha önce bu analizi gerçekleştirmiş olan kişilerin yorumlarını da inceleyebilirsiniz.

Bu e-posta, alışılmadık bir alan adıyla gelen şüpheli bir mesaj olarak tespit edilmiştir. Ancak, yapılan detaylı analizler sonucunda, söz konusu alan adının kötü amaçlı bir tehdit içermediği ve geçmişte zararlı etkinliklerle ilişkilendirilmediği doğrulanmıştır. Tüm incelemeler, bu alarmın false positive olduğunu göstermektedir. Bu nedenle ilgili kayıt False Positive olarak işaretlenip kapatılmıştır.

Alarm Bilgisi ID:1001

1001 numaralı ID ye sahip alarmı incelediğimizde bazı bilgiler görmekteyiz.



Kuruluşa ait güvenlik sistemleri tarafından alışılmadık bir üst düzey etki alanına sahip harici bir göndericiden gelen şüpheli bir e-posta tespit edilmiştir. E-posta, 'VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping' konulu bir mesaj içeriyordu ve gönderici, chicmillinerydesigns.de alan adını kullanan Maximillian olarak görünüyor.

Bu e-posta, chicmillinerydesigns.de alan adını kullanarak Michelle Smith'e gönderilmiş olup, harici bir kaynaktan içeriye doğru yönlendirilmiştir.

SOC Başkanı tarafından yapılan değerlendirmeye göre, bu tespit kuralının ince bir ayara ihtiyacı olabilir veya hâlâ geliştirilmesi gerekmektedir. Bu bilgiye description bölümünden ulaştığımızı söyleyebiliriz. Bu da, e-postanın false-positive olma ihtimalini düşündürmektedir.

Olayın tam zaman bilgisi, 03/01/2025 08:40:40.125 zaman damgası (timestamp) ile kaydedilmiştir.

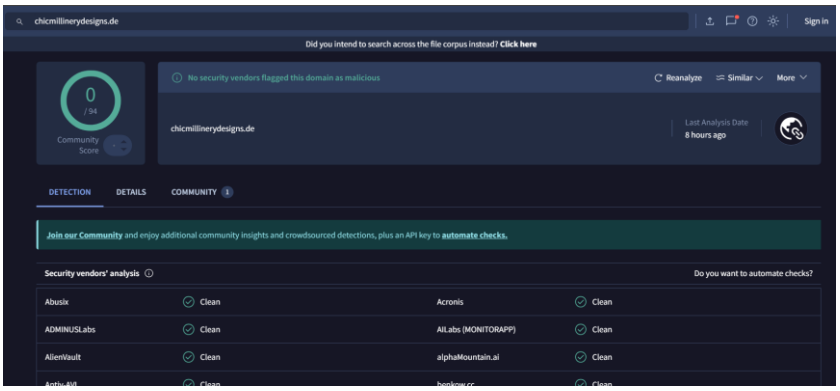
Ayrıca, e-postanın içeriği gizlilik düzenlemeleri ve güvenlik politikaları gereği kaldırılmış olup, herhangi bir ek içermediği tespit edilmiştir.

Alarm İncelemesi ID:1001

İlgili alarmı incelediğimizde, 1000 numaralı ID'ye sahip alarmda olduğu gibi, e-posta üzerinde aynı metodolojinin uygulandığını görebiliyoruz. Bu yüzden, aynı şekilde analiz için sadece elimizde bir alan adı bulunmaktadır.

Aynı şekilde sırasıyla AnyRun ve VirüsTotal üzerinde sorgulatma sağlıyoruz.

Görüldüğü üzere VirüsTotal üzerinde sorgulatma sağladığımızda güvenli görünmektedir.



AnyRun üzerinde sorgulatıldığında ise analistler tarafından yürütülen oturum analizlerinden birini görüntülüyoruz, burada da herhangi bir tehdit tespit edilmediğinin bilgisini alıyoruz.

Yapılan analizler sonucunda söz konusu alan adının kötü amaçlı bir tehdit içermediği ve geçmişte zararlı etkinliklerle ilişkilendirilmediği doğrulanmıştır. Tüm incelemeler, bu alarmın false positive olduğunu göstermektedir. Bu nedenle ilgili kayıt False Positive olarak işaretlenip kapatılmıştır.

Alarm Bilgisi ID:1002

1002 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.

Burada ortam üzerinde tespit edilen alışılmadık bir işlem ilişkisini görünmektedir. Alışılmadık parent-child ilişkisi, bir parent işleminin garip bir şekilde başka bir işlem veya sistem işlemi başlatması ve bunun sistem dışı bir işlem tarafından yanıtlanması durumudur. Bu tür ilişkiler alışılmadık parent-child ilişkisi olarak adlandırılır.

İncelediğimiz işlemde, taskhostw.exe işlem kimliği 3897 olan bir işlem, svchost.exe işlem kimliği 3902 olan bir sistem işlemi tarafından başlatılmış. Komut satırı taskhostw.exe NGCKeyPregen olarak belirtilmiş ve işlem çalışma dizini *C:\Windows\system32* olarak tespit edilmiştir.

Bu durum, yazılımı kötüye kullanmak veya zararlı bir işlem yapmak amacıyla başlatılan bir işlem olabilir. Şimdi, bu iki işlem arasındaki ilişkiyi incelemeli ve yaygın bir durum olup olmadığını belirlemeliyiz.

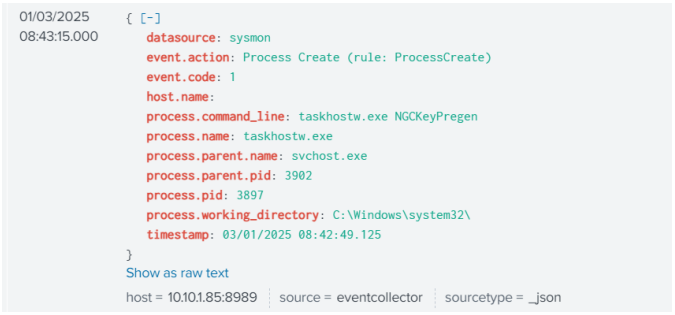
Alarm İncelemesi ID:1002

Bu durum, yazılımı kötüye kullanmak veya zararlı bir işlem yapmak amacıyla başlatılan bir işlem olabilir. Şimdi, bu iki işlem arasındaki ilişkiyi incelemeli ve yaygın bir durum olup olmadığını belirlemeliyiz. Öncelikle process pid 3897 olduğunu biliyoruz.

Splunk kullanarak daha ayrıntılı bir inceleme gerçekleştirebiliriz. İlk olarak işlem kimliği 3897'yi kullanarak bir sorgulama yapıyoruz. İşlem kimliğimizin 3897 olduğunu gözlemliyoruz ve bu doğrultuda Splunk üzerinde **"process.pid"=3897** şeklinde bir arama yapıyoruz.

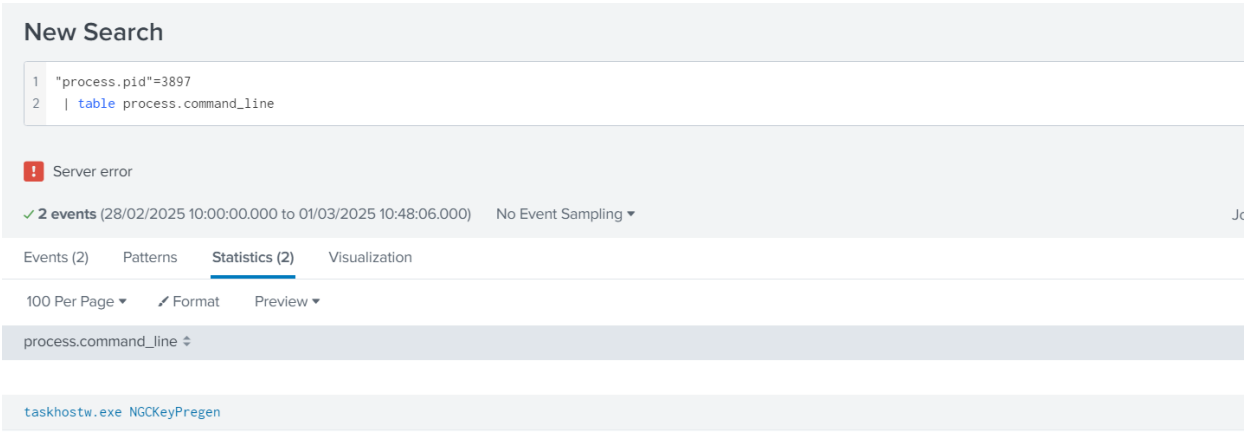
```
1 process.pid="3897"
```

Sorgulama sonucunda, daha önce tespit ettiğimiz aynı olayla karşılaşıyoruz. Burada hizmet sunucusu, görev sunucusunu başlatmaktadır. Yapmamız gereken bir sonraki adım bu veriyi daha derinlemesine incelemek ve sonuçları tablo formatında düzenlemektir.



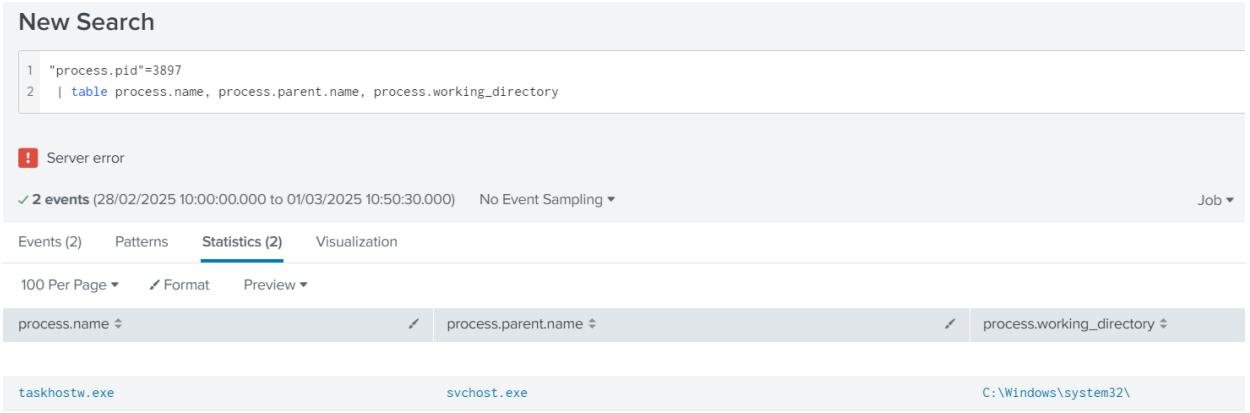
"process.pid"=3897

| table process.command_line sorgusunu çalıştırıyoruz. Bu sorgunun amacı, ilgili işlemle ilişkilendirilmiş komut satırını elde etmektir. Çıktı olarak **taskhostw.exe NGCKeyPregen** bilgisi yer almaktadır.



"process.pid"=3897

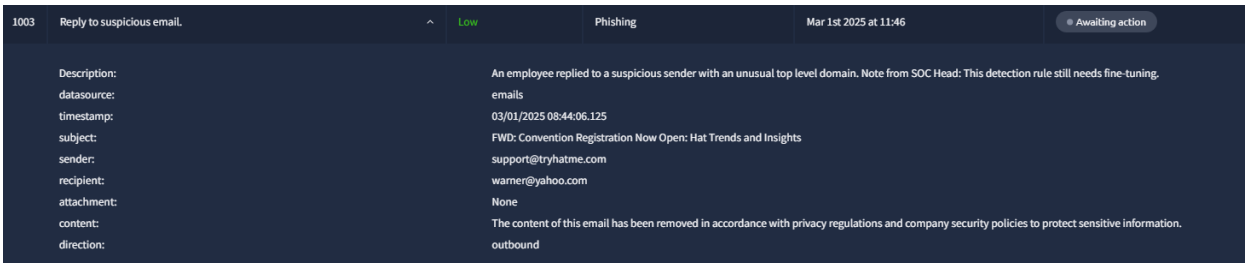
| table process.name, process.parent.name, process.working_directory sorgusunu çalıştırıyoruz. Bu sorguyla, işlem adı, parent işlem adı ve çalışma dizini gibi ek bilgilere ulaşmayı hedefliyoruz. Elde ettiğimiz sonuçlara göre, işlem adı taskhost.exe, parent işlem adı svchost.exe ve çalışma dizini *C:\Windows\system32* olarak belirlenmiştir.



Bu parent-child ilişkisini incelediğimizde, bunun alışılmadık bir durum olmadığını görmekteyiz. Bu ilişki sistemin normal işleyişiyle uyumludur çünkü system32 dizini, Windows işletim sistemine ait orijinal yürütülebilir dosyaların bulunduğu bir dizindir. svchost.exe, temel bir hizmet sunucusu olup görev zamanlayıcı hizmetini yöneten taskhost.exe'yi başlatmaktadır. Bu nedenle svchost.exe tarafından taskhost.exe'nin başlatılması, sistemin normal çalışma sürecinin bir parçasıdır. Sonuç olarak, bu ilişkilerin alışılmadık olmadığını ve yaygın olduğunu tespit etmekteyiz. Alarm false-positive olarak kapatılmıştır.

Alarm Bilgisi ID:1003

1003 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.



Kuruluşa ait güvenlik sistemleri, alışılmadık bir üst düzey etki alanına sahip şüpheli bir göndericiye yanıt veren bir çalışanı tespit etmiştir.

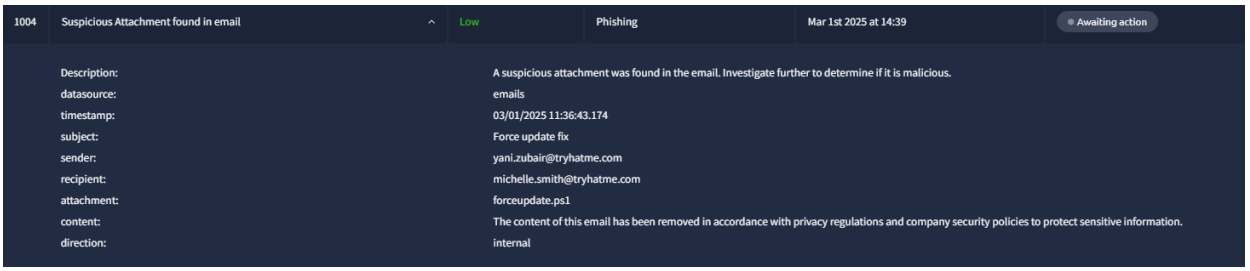
SOC Başkanı tarafından yapılan değerlendirmeye göre, bu tespit kuralı hâlâ ince ayar gerektirmektedir. Bu durumda, bir dışa çıkış işlemi söz konusudur. Yani kuruluş içinden bir kişi, kuruluşun etki alanı dışında bulunan birine e-posta göndermek üzere bir yanıt vermiştir.

Gönderici olarak support@tryhatme.com, alıcı olarak ise warner@yahoo.com adresi yer almaktadır. E-postanın konusu "FWD: Convention Registration Now Open: Hat Trends and Insights" şeklindedir.

Bu durumda, bir kuruluş çalışanı yahoo.com adresine yanıt vermiştir. Yahoo.com alan adı doğru ve yazım hatası içermemektedir. Bu da gösteriyor ki e-posta aslında geçerli bir adresle gönderilmiş olup bu durum bir false positive olarak değerlendirilebilir. Alarm false- positive olarak kapatılmıştır.

Alarm Bilgisi ID:1004

1004 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.



İnceleme sağladığımızda bu e-posta, içeriğinde şüpheli bir ek dosya barındırmaktadır. E-posta, şirket içi bir kullanıcı tarafından başka bir şirket içi kullanıcıya gönderilmiş, bu da iletişimin "internal" olduğunu gösteriyor. E-postanın konusu "Force update fix" ve ek olarak forceupdate.ps1 adlı bir PowerShell betiği (PS1 dosyası) bulunuyor. Bu tür dosyalar genellikle sistemdeki güncellemeler veya düzeltmeler için kullanılsa da kötü niyetli yazılımlar tarafından da kötüye kullanılabilir.

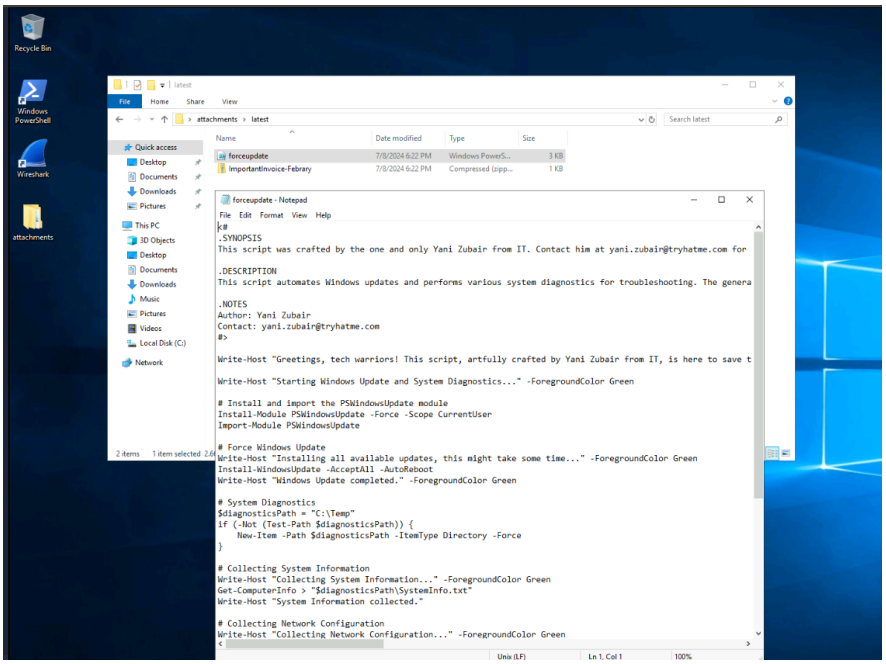
E-posta içeriği gizlilik düzenlemeleri ve güvenlik politikaları nedeniyle kaldırılmış, bu da sadece ekin dikkatlice incelenmesi gerektiğini bir kez daha vurguluyor. PS1 uzantılı dosyalar, kötü amaçlı yazılımlar için yaygın bir taşıyıcı olabilir çünkü PowerShell betikleri genellikle sistem üzerinde komutlar çalıştırmak için kullanılır.

Bu durumda, ekin zararlı olup olmadığını belirlemek için ayrıntılı bir inceleme yapılması gerekir. Forceupdate.ps1 dosyasının içeriği, kim tarafından ve nasıl oluşturulduğu, çalıştırılmaya başladığında sistem üzerinde yaptığı işlemler gibi faktörler göz önünde bulundurulmalıdır. Ayrıca e-postadaki gönderen ve alıcı bilgileri de kontrol edilerek bu tür bir iletişimin güvenli olup olmadığı değerlendirilebilir.

Alarm İncelemesi ID:1004

E-postada şüpheli bir ek dosya bulundu ve bu dosyanın kötü amaçlı olup olmadığını belirlemek için daha fazla inceleme yapılması gerektiği belirtilmiştir. E-posta, yani.zubair@tryhatme.com adresinden gönderilmiş olup, alıcı michelle.smith@tryhatme.com'dur. Konusu "Force update fix" olarak belirtilmiştir ve ektedir bir komut dosyası (forceupdate.ps1) yer almaktadır.

Bu durumda, şüpheli ek dosyayı analiz etmek için ilgili VM ortamına gidilmesi gerektiği anlaşılmaktadır. "Forceupdate.ps1" dosyasını, ekler klasöründe görüntüleyerek, Not Defteri ile açıyoruz. Dosya içeriği incelendiğinde bu komut dosyasının Windows sorunlarını tanıyan ve gideren bir script olduğu görülmektedir. Ayrıca, PSWindowsUpdate modülünü yükleyip içe aktararak Windows güncellemelerini zorla gerçekleştirdiği görülmektedir.



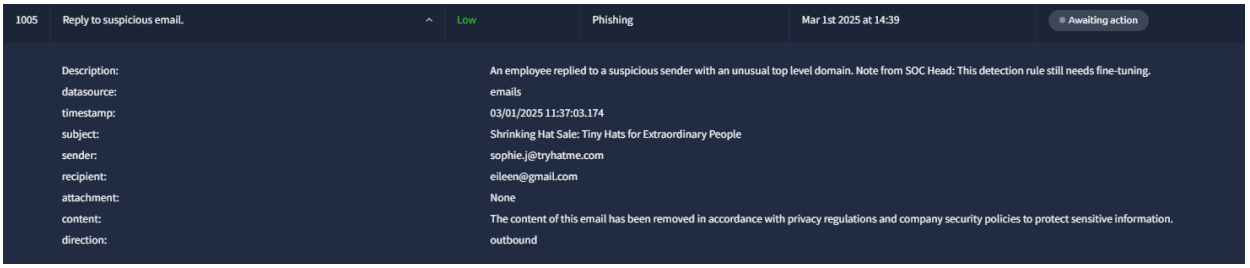
İlk satırda, Windows güncellemelerini zorla yükleyip, otomatik yeniden başlatmayı kabul eden komutlar yer alırken, bir sonraki satırlarda ise sistem tanılama işlemi başlatılmaktadır. Komut dosyası, Windows'taki geçici dizine sistem bilgilerini toplayarak, Get-ComputerInfo komutunu çalıştırmakta ve bu verileri belirtilen dosyaya kaydetmektedir. Aynı şekilde ağ yapılandırmasını toplayıp, çıktıyı ağ yapılandırma dosyasına kaydederek benzer bir işlem yapılmaktadır. Yüklü programlar da toplanmakta ve sonuçlar geçici olarak kaydedilmektedir.

```
# Install and import the PSWindowsUpdate module
Install-Module PSWindowsUpdate -Force -Scope CurrentUser
Import-Module PSWindowsUpdate

# Force Windows Update
Write-Host "Installing all available updates, this might take some time..." -ForegroundColor Green
Install-WindowsUpdate -AcceptAll -AutoReboot
Write-Host "Windows Update completed." -ForegroundColor Green

# System Diagnostics
$diagnosticsPath = "C:\Temp"
if (-Not (Test-Path $diagnosticsPath)) {
    New-Item -Path $diagnosticsPath -ItemType Directory -Force
}
```

Tüm bu işlemler tamamlandıktan sonra tanılama dosyaları saklanmakta ve son olarak e-posta ile mesaj gönderilmektedir. Genel olarak, komut dosyası, sistem tanılaması ve güncelleme işlemlerini gerçekleştiriyor gibi görünmektedir. Komut dosyası detaylı incelenmiş olup tehdit tespit edilmemiştir. Bu yüzden false-positive olarak kapatılmıştır.

Alarm Bilgisi ID:1005

1005 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.



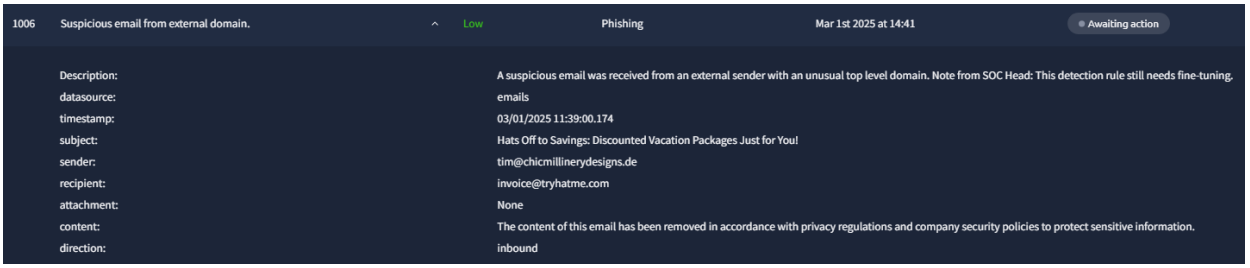
Bir çalışan alışılmadık bir üst düzey etki alanına sahip şüpheli bir göndericiye yanıt vermiştir. E-posta, sophie.j@tryhatme.com adresinden gelmiş ve eileen@gmail.com adresine yönlendirilmiştir.

E-posta başlığı ise "Shrinking Hat Sale: Tiny Hats for Extraordinary People" şeklindedir. E-postanın içeriği, gizlilik düzenlemeleri ve şirket güvenlik politikaları gereği kaldırılmıştır. E-posta herhangi bir ek içermemektedir.

Alan adlarının kontrolü yapıldığı için alarm false-positive olarak değerlendirilmiş olup kapatılmıştır.

Alarm Bilgisi ID:1006

1006 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.



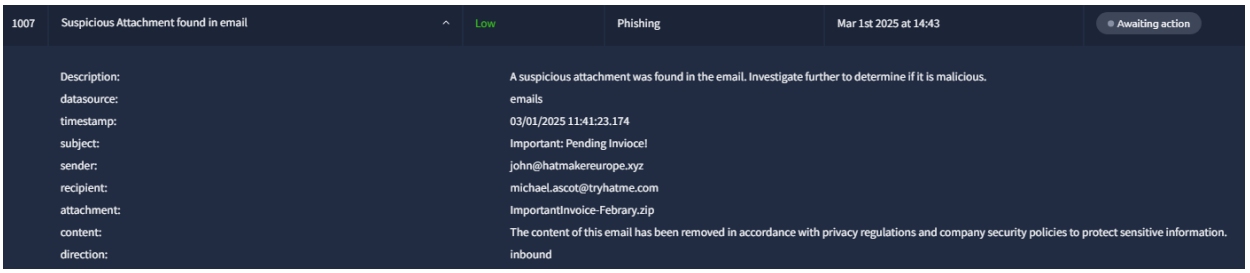
Alışılmadık bir üst düzey etki alanına sahip harici bir göndericiden şüpheli bir e-posta alınmıştır. E-posta, tim@chicmillinerydesigns.de adresinden gönderilmiş olup, invoice@tryhatme.com adresine yönlendirilmiştir. E-posta başlığı "Hats Off to Savings: Discounted Vacation Packages Just for You!" şeklindedir. E-posta içeriği, gizlilik düzenlemeleri ve şirket güvenlik politikaları gereği kaldırılmıştır ve herhangi bir ek içermemektedir.

SOC Başkanı'nın eklediği nota istinaden bu tespit kuralı hâlâ ince ayar gerektirmektedir, bu nedenle bu e-posta üzerinde daha fazla analiz yapılması gerektiği belirtilmiştir. Şüpheli gönderenin chicmillinerydesigns.de etki alanı, alışılmadık bir alan adı kullanması nedeniyle bu durumun false-positive olma olasılığını düşündürmektedir. Bu tür e-postaların dikkatle incelenmesi önemlidir.

Ancak daha önce analiz edilen chicmillinerydesigns.de alan adı üzerinde yapılan çalışmalar, bu alanın kötü amaçlı olmadığını göstermiştir. Bu nedenle, bu e-posta göndericisinin gerçekten bir çalışanımız olduğunu ve e-posta içeriğinin güvenli olduğunu belirtiyoruz. Ayrıca, e-posta herhangi bir ek içermemektedir, bu da e-postanın güvenli olduğunu gösterir. Sonuç olarak bu olayın bir false-positive olduğunu ve herhangi bir tehdit teşkil etmediğini söyleyebiliriz.

Alarm Bilgisi ID:1007

1007 numaralı ID ye sahip ilk alarmı incelediğimizde bazı bilgiler görmekteyiz.



Bu kayıtta, harici bir göndericiden gelen şüpheli bir e-posta tespit edilmiştir. E-posta john@hatmakereurope.xyz adresinden michael.ascot@tryhatme.com adresine gönderilmiş olup başlık "Important: Pending Invoice!" şeklindedir. E-postanın ekinde ise ImportantInvoice-Febrary.zip adlı bir dosya bulunmaktadır.

Bu durumda e-posta ekinin içeriği potansiyel olarak zararlı olabilir ve dikkatlice incelenmesi gerekmektedir. Dosya adı genellikle fatura gibi resmi bir belgeyi çağrıştırıyor olsa da, uzantısının zip olması dosyanın bir sıkıştırılmış dosya olduğunu ve içeriğinin bilinmeyen yazılımlar ya da kötü amaçlı kodlar taşıyor olabileceğini düşündürebilir.

Bu nedenle dosyanın içeriğini incelemek için güvenli bir ortamda açılması ve detaylı bir şekilde taranması gerekmektedir.

Alarm İncelemesi ID:1007

Öncelikle Analist VM'ini açtıktan sonra, attachment klasöründeki ImportantInvoice-Febrary.zip dosyasını dikkatlice dışarıya ayıklıyoruz. Analist makinesinde bulunduğumuz için, örnekleri çıkarmak veya açmak sorun teşkil etmiyor. Klasörü ayıkladığımızda bir PDF dosyasıyla karşılaşıyoruz. Şimdi bu PDF dosyasını analiz etmek için önce hash değerini almak üzere PowerShell'i kullanarak dosyanın karma değerlerine ulaşmamız gerekiyor.

Get-FileHash komutunu kullanarak bir dosyanın hash (karma) değerini alabiliriz. Bu, dosyanın içeriğine dayanarak benzersiz bir dijital parmak izi oluşturur. Bu işlem dosyanın değiştirilip değiştirilmediğini doğrulamak ve şüpheli dosyaları analiz etmek için oldukça önemlidir. Şimdi, invioce.pdf.lnk dosyasının iki farklı hash değerini nasıl alacağımızı detaylandırarak açıklayalım.

SHA256, güvenli bir şifreleme algoritmasıdır ve 256 bitlik bir hash değeri üretir. Bu değeri almak için şu komutu kullanıyoruz. **Get-FileHash .\invioce.pdf.lnk**

```
PS C:\Users\Administrator\desktop\attachments\latest\ImportantInvoice-Febrary> Get-FileHash .\invioce.pdf.lnk

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          50E5BF8361DF2442546F21E08B1561273F4CCC610258F622AC1A4B8EBF0A0386       C:\Users\Administrator\deskto...

PS C:\Users\Administrator\desktop\attachments\latest\ImportantInvoice-Febrary>
```

SHA256:
50E5BF8361DF2442546F21E08B1561273F4CCC610258F622AC1A4B8EBF0A0386

MD5, daha kısa bir 128 bitlik hash değeri üretir ve genellikle daha hızlı bir algoritma olarak kullanılır. Ancak, güvenlik açısından daha eski bir algoritma olduğundan günümüzde daha güvenli alternatifler tercih edilmektedir. MD5 hash değerini almak için şu komutu kullanıyoruz:

Get-FileHash .\invioce.pdf.lnk –Algorithm MD5

```
PS C:\Users\Administrator\desktop\attachments\latest\ImportantInvoice-Febrary> Get-FileHash .\invioce.pdf.lnk -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             ED1DC2D678743FCBEDF0D743E27D0362                                       C:\Users\Administrator\desktop\attachments\latest\ImportantInvoice-Febrary\invioce.pdf.lnk

PS C:\Users\Administrator\desktop\attachments\latest\ImportantInvoice-Febrary>
```

MD5: ED1DC2D678743FCBEDF0D743E27D0362

SHA256 ve MD5 hash değerlerini ANYRUN ve VirusTotal üzerinden sorgulattığımızda herhangi bir çıktı almadık. Bu durum dosyanın zararsız olduğu anlamına gelmez çünkü her iki platform da yalnızca daha önce bilinen kötü amaçlı yazılımlar ve şüpheli dosyalarla ilgili veritabanlarında bulunan hash değerlerini gösterir. Eğer dosya yeni veya daha önce hiç analiz edilmemiş bir dosya ise bu tür araçlar üzerinde herhangi bir sonuç almayabiliriz.

Bu analizde, Splunk kullanarak günlüklerle veya olaylarla ilişkilendirme yapmamız gerektiği sonucuna varıyoruz. Örneğin fatura adı veya dosya adı üzerinden arama yapabiliriz. Buradaki uyarı, belirli bir ek ile gönderilen e-posta ile ilgili ve dosya adı "invoice.pdf.lnk" olarak belirlenmiş. Bu dosya adı üzerinden arama yaparak, dosyanın gerçekten açılıp açılmadığını ve açıldıktan sonra ne tür bir işlem gerçekleştiğini araştırmamız önemli.

Dosyanın adını kullanarak Splunk üzerinden arama yapmamız gerekiyor. Burada "invoice.pdf.lnk" dosyasını kopyalayarak aramayı başlatıyoruz. Amacımız, bu faturanın açılıp açılmadığını ve açıldıktan sonra hangi işlemlerin gerçekleştiğini bulmak. Bu tür bir arama ile, dosyanın kötü amaçlı olup olmadığını anlamaya çalışacağız.

i	Time	Event
›	01/03/2025 12:02:13.000	{ [-] datasource: sysmon event.action: File stream created (rule: FileCreateStreamHash) event.code: 15 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5\Temp1_ImportantInvoice-Febrary.zip\ImportantInvoice-Febrary\invioce.pdf.lnk host.name: win-3450 process.name: Explorer.EXE process.pid: 3180 timestamp: 03/01/2025 12:01:41.174 } Show as raw text host = 10.10.239.8:8989 source = eventcollector sourcetype = _json
›	01/03/2025 12:01:42.000	{ [-] datasource: sysmon event.action: File stream created (rule: FileCreateStreamHash) event.code: 15 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5\Temp1_ImportantInvoice-Febrary.zip\ImportantInvoice-Febrary\invioce.pdf.lnk host.name: win-3450 process.name: Explorer.EXE process.pid: 3180 timestamp: 03/01/2025 12:01:41.174

Kayıtlar incelendiğinde faturanın açılmış olduğunu görüntülüyoruz. Faturayı açmış olmakta bu dosyanın zararlı olduğu anlamına gelmez. Kayıtların tamamı incelendiğinde ise yürütülebilir komut dosyalarının çalıştırıldığını görüntülüyoruz. Alarm true-positive olarak değerlendirilmiş olup kapatılmıştır.