Splunk — Boss of the SOC v1

11 Mayıs 2024 tarihinde BTK'nın Siber Tehdit İstihbaratı ve Olay Müdahale Atölyesi'nde öğrendiğim Splunk Bots çözümlerini sizlerle paylaşmak istiyorum. İyi okumalar dilerim.

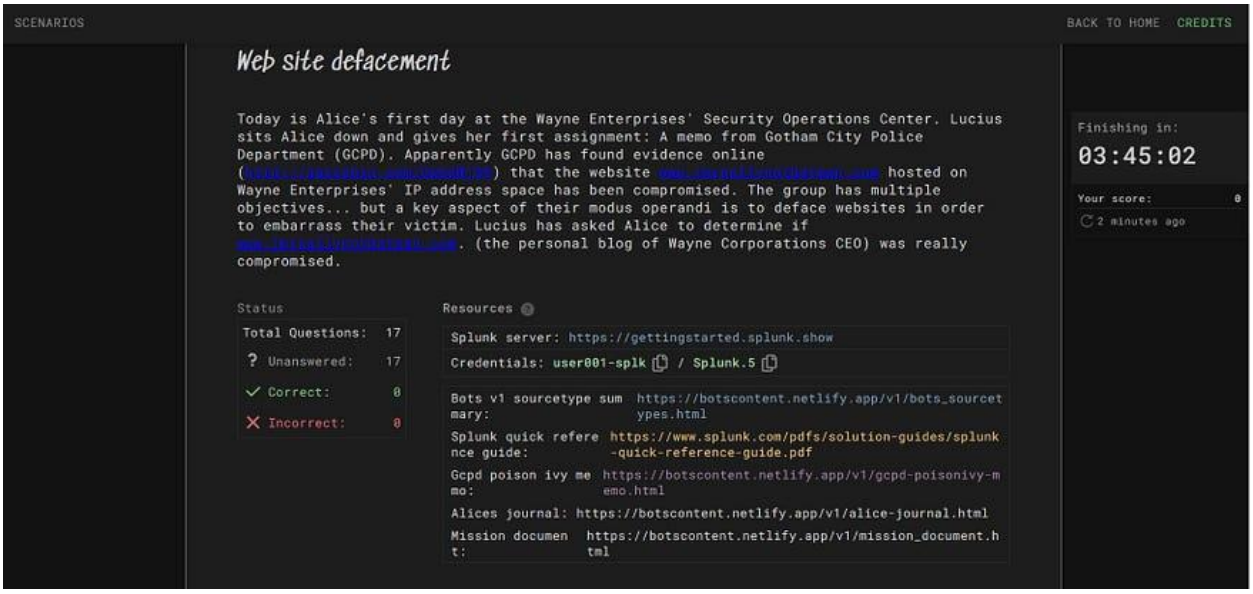
Önce Splunk'ın ne olduğundan başlayalım.

Splunk, büyük veri analizi ve izleme için kullanılan bir platformdur. Çeşitli kaynaklardan gelen verileri toplar, depolar, analiz eder ve görselleştirir. İşletmelere BT altyapısının performansını artırmak, sorun giderme yapmak ve güvenlik sağlamak için yardımcı olur.

Splunk bots ise, Splunk platformunun otomasyon yeteneklerini genişletmek için kullanılan önceden yapılandırılmış ve programlanmış botlardır. Bu botlar, belirli görevleri gerçekleştirmek için yapılandırılmıştır ve Splunk Enterprise veya Splunk Cloud gibi Splunk ürünleriyle entegre çalışabilirler. Splunk botları, kullanıcıların manuel olarak yapması gereken tekrarlayan görevleri otomatikleştirmelerine ve Splunk platformunun kullanımını daha verimli hale getirmelerine yardımcı olabilir.

Şimdi Google'a splunk bots yazarak başlayabiliriz. İlk çıkan siteye tıklayıp üyelik oluşturarak kaydımızı tamamlıyoruz.

Play Now'dan Boss of the SOC Version 1'e tıklayıp 1. senaryo olan Web Site Defacement'i seçiyoruz.



Splunk server'a tıklayarak verilen username ile password'u giriyoruz. Daha sonra soruları açıyoruz.

Bu arada bu senaryoda toplam 17 soru var. Bugün ben sadece 101, 102, 104 ve 109. soruları çözdüm. Ayrıca her sorunun puanı olup yanlış girilen cevaplar da -10 puan olarak hesaplanıyor.

#101

Question:

What is the likely IPv4 address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?

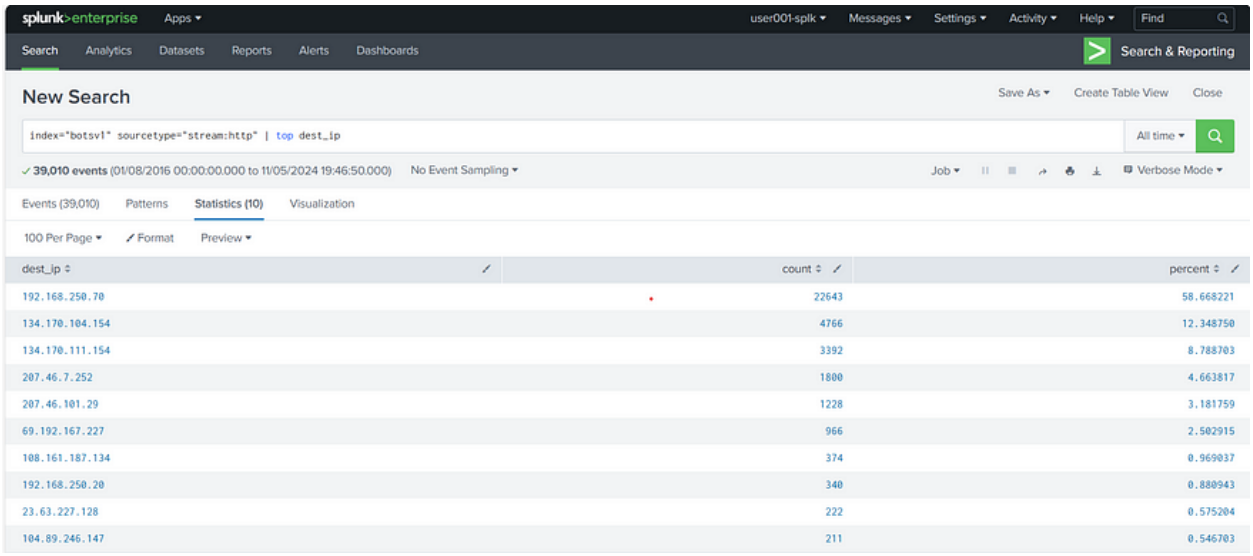
Öncelikle,

index="botsv1" sourcetype="stream:http" | top dest_ip

sorgusunu yazıyorum.

Bu SPL yani Splunk Processing Language sorgusu, "botsv1" dizinindeki ve "stream:http" kaynak türündeki verileri filtreler. Sonra bu verileri "dest_ip" alanına göre gruplar ve her bir IP adresinin ne kadar sık kullanıldığını sayar. Sonuç olarak, en çok hit alan IP adresini bulur.

Ve bu sorgudan 192.168.250.70 IP'yi öğreniyoruz.

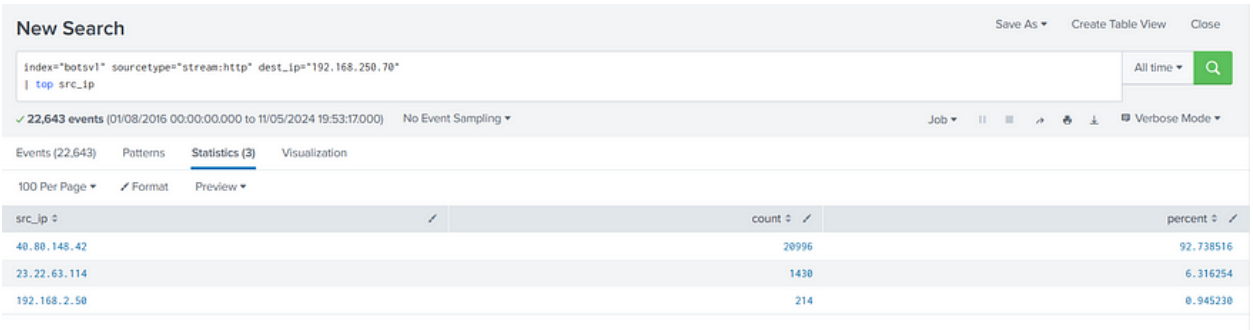


Daha sonra;

index=”botsv1" sourcetype=”stream:http” dest_ip=”192.168.250.70"
| top src_ip

komutunu yazıyorum.

Bu sorgu, “botsv1” dizinindeki ve “stream:http” kaynak türündeki verileri filtreler. Bu filtreleme, belirli bir “dest_ip” (hedef IP adresi) değerine sahip olan kayıtları içerir, yani 192.168.250.70. Daha sonra, bu filtrelenmiş veriler “src_ip” (kaynak IP adresi) alanına göre gruplanır ve her bir kaynak IP adresinin kaç kez kullanıldığını sayar. Sonuç olarak, en çok hit alan kaynak IP adresini bulur.



Cevap 40.80.148.42

#102

Question:

What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name.

Answer guidance: For example “Microsoft” or “Oracle”

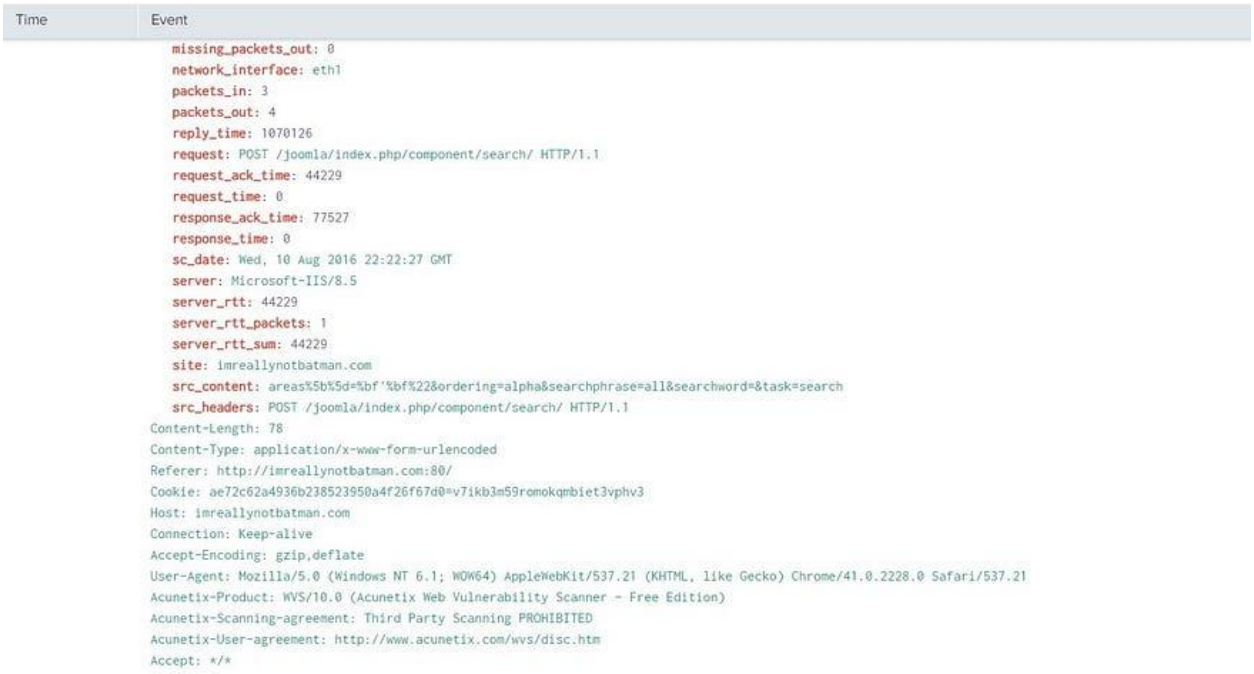
İlk önce;

index=”botsv1" sourcetype=”stream:http” dest_ip=”192.168.250.70" src_ip=”40.80.148.42"

sorgusunu yazıyorum.

Bu sorgu, belirli bir hedef IP adresine (192.168.250.70) yapılan isteklerin kaynak IP adresi (40.80.148.42) ile ilişkili olanlarını belirlemek için kullanılır. Yani, 40.80.148.42 IP adresinden gelen isteklerin, 192.168.250.70 IP adresine yönlendirildiği kayıtları bulmak için bu sorgu kullanılır.

Ya da ilk soru için de kullanabileceğimiz index=”botsv1" “imreallynotbatman.com” sorgusunu şu an da tekrar yazarak aratıyorum. Biraz göz gezdirdikten sonra kullanılan web güvenlik açığı tarayıcısını oluşturan şirketin Acunetix olduğu anlaşılıyor .



Cevap: Acunetix

#104

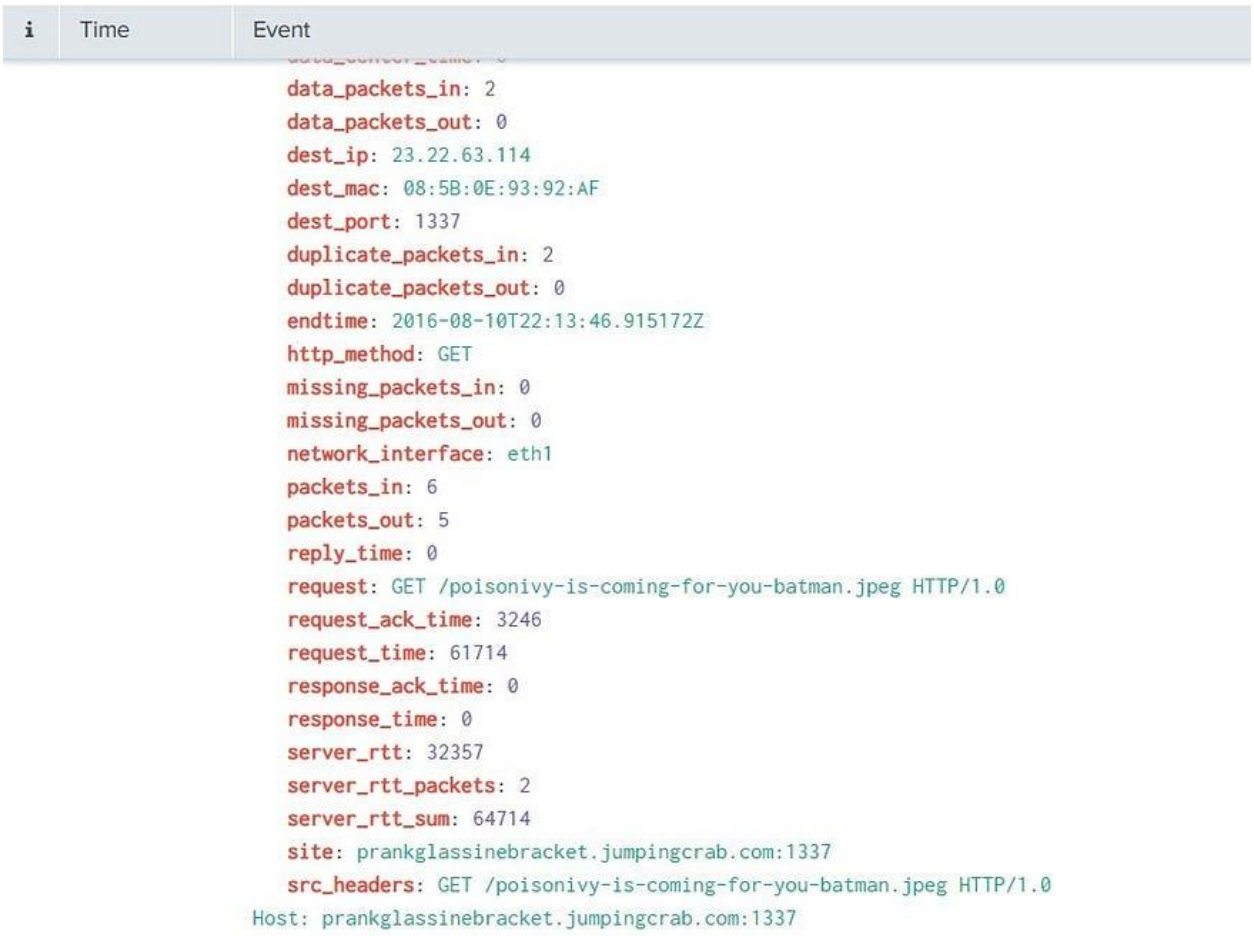
Question:

What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with extension?

Sunucumuzun kaynak IP adresinin kötü amaçlı bir dosyayı indirdiğini varsayarsak ve bu indirme işlemlerinin HTTP GET yöntemini kullandığını biliyorsak, bu bilgilerle birlikte ilgili verileri analiz edebiliriz. Aşağıdaki sorgu, sunucumuzun belirli bir zaman aralığında belirli bir dosyayı indirip indirmediğini kontrol etmek için kullanılabilir. Bu sorguyu çalıştırarak sunucumuzun faaliyetlerini inceleyebilir ve herhangi bir şüpheli veya ilginç etkinlik bulabiliriz.

index=”botsv1" sourcetype=”stream:http” src_ip=”192.168.250.70"

yazıp sonuna da http_method=GET ekleyebiliriz.



Sonuçlara göz attığımızda, “poisonivy-is-coming-for-you-batman.jpeg” adlı dosya için kullanılan HTTP GET yöntemine atıfta bulunan bir istek alanı içerdiğini görüyoruz.

Cevap: poisonivy-is-coming-for-you-batman.jpeg

#109

Question:

What is the name of the executable uploaded by Po1s0n1vy?

Answer guidance: Please include file extension. (For example, “notepad.exe” or “favicon.ico”)

Tehdit aktörünün IP adresinin 40.80.148.42 olduğunu biliyoruz ve bir tür çalıştırılabilir dosya arıyoruz. Bildiğimiz bilgilere dayanarak aşağıdaki SPL sorgusunu oluşturabiliriz ve genellikle çalıştırılabilir dosya uzantısı olan .exe için bir yıldız * ekleyebiliriz.

index=”botsv1" src_ip=”40.80.148.42" *.exe* ya da

index=”botsv1" dest_ip=”192.168.250.70" *.exe* POST

sorgularını denedim.

Bu SPL sorgusu, belirli bir IP adresine (192.168.250.70) yapılan istekler arasından, dosya adında “.exe” uzantısı bulunan ve HTTP POST yöntemiyle gönderilen istekleri bulur. Bu, belirli bir IP adresinden gelen ve muhtemelen kötü amaçlı yazılım veya zararlı dosyaların dağıtımını hedefleyen istekleri izlemek için kullanılır.

Gelen sonuçları incelerken show as raw text’e tıkladım ve cevabı orada gördüm.

Cevap: 3791.exe