

Analitik SQL

Yusuf Eymen TAKAK
eymen.takak@bilgiedu.net



SQL (Structured Query Language)

ilişkisel veritabanı yönetim sistemlerinde (RDBMS) veri tabanlarına erişmek, veri manipülasyonu ve veri tanımlama işlemleri için kullanılan bir programlama dilidir. SQL, kullanıcıların veritabanıyla etkileşimde bulunmalarını sağlar.

SQL, veritabanında saklanan verilere erişmek için kullanıcıların sorgularını göndermelerine izin verir. Bu sorgular, veritabanından veri alma, veri ekleme, veri güncelleme ve veri silme gibi işlemleri gerçekleştirebilir. SQL, standart bir dil olarak kabul edilir ve birçok veritabanı yönetim sistemi tarafından desteklenir.



ANALİTİK SQL

SQL dilini kullanarak veri analizi yapmak için tasarlanmış bir yaklaşımdır. Veri analizi, büyük miktarda veriyi anlama, keşfetme ve değerlendirme sürecidir. Analitik SQL, gelişmiş sorgu ve analiz tekniklerini kullanarak veritabanında depolanan verileri analiz etmeyi sağlar.

Analitik SQL, geleneksel SQL sorgularına ek olarak daha karmaşık analiz ve hesaplama işlemlerini gerçekleştirmek için özel işlevler ve operatörler sunar. Örneğin, bir veri kümesi üzerinde istatistiksel hesaplamalar yapmak, verileri gruplandırmak, sıralamak, filtrelemek veya birleştirmek gibi işlemler analitik SQL kullanılarak gerçekleştirilebilir. Analitik SQL, iş zekası (business intelligence) ve veri analitiği gibi alanlarda kullanılır. Büyük veri kümelerini analiz etmek ve anlamlı bilgiler elde etmek için kullanıcıların veritabanı üzerinde kompleks sorguları çalıştırmasına olanak sağlar. Ayrıca, verileri raporlama veya görselleştirme araçlarına aktarmak için de kullanılabilir.

Analitik SQL ve SQL arasındaki temel farklar

Veri Manipülasyonu ve Analiz Yetenekleri	İşlem Amaçları
İşlem Miktarı ve Veri Boyutu	Sorgu Karmaşıklığı
Performans Optimizasyonu	Veri Yapıları ve Modelleri
Karmaşık Analitik İşlevler	Veri Kaynakları

İŞLEM MIKTARI VE VERİ BOYUTU

SQL genellikle tek bir tabloya veya küçük veri kümelerine yönelik işlemleri gerçekleştirmek için kullanılır. Analitik SQL ise daha büyük veri kümeleriyle çalışır ve genellikle veri analizi ve iş zekası projelerinde kullanılır. Analitik SQL, büyük veri tabanlarında kompleks sorguları çalıştırarak geniş çaplı analizler yapabilir.

VERİ MANİPÜLASYONU VE ANALİZ YETENEKLERİ

SQL, veritabanı işlemleri için kullanılan bir dil olarak temel veri ekleme, güncelleme, silme ve sorgulama işlemlerini gerçekleştirmek için kullanılır. Analitik SQL ise, SQL'nin temel işlevlerini genişleterek veri analizi için özel analiz fonksiyonları ve operatörler sağlar. Analitik SQL, verileri filtrelemek, gruplandırmak, sıralamak, birleştirmek, istatistiksel hesaplamalar yapmak gibi daha karmaşık analiz ve hesaplama yetenekleri sunar.

İŞLEM MIKTARI VE VERİ BOYUTU

SQL genellikle tek bir tabloya veya küçük veri kümelerine yönelik işlemleri gerçekleştirmek için kullanılır. Analitik SQL ise daha büyük veri kümeleriyle çalışır ve genellikle veri analizi ve iş zekası projelerinde kullanılır. Analitik SQL, büyük veri tabanlarında kompleks sorguları çalıştırarak geniş çaplı analizler yapabilir.

PERFORMANS OPTIMİZASYONU

Analitik SQL, büyük veri kümelerini analiz etmek için optimize edilmiş performans teknikleri kullanır. Örneğin, analitik SQL, verileri paralel işleme tabi tutarak sorgu performansını artırabilir. SQL ise genellikle daha küçük veri kümeleri üzerinde çalıştığından performans optimizasyonu genellikle daha küçük ölçekte yapılır.

KARMAŞIK ANALITIK İŞLEVLER

Analitik SQL, özel analistik işlevlere ve operatörlere sahiptir. Bu işlevler, istatistiksel hesaplamalar, trend analizi, veri madenciliği, tahmin yapma gibi analitik işlemleri gerçekleştirmek için kullanılabilir. SQL ise daha temel veri manipülasyon işlemlerine odaklanır.

VERİ YAPILARI VE MODELLERI

SQL, ilişkisel veritabanları için tasarlanmıştır ve tablolar arasında ilişkiler kullanarak verileri düzenler. Bu ilişkisel veri modeli, verilerin tutarlığını ve bütünlüğünü sağlamak için kısıtlamalar ve ilişkiler içerir. Analitik SQL ise, genellikle daha karmaşık veri yapılarına ve modellere uygulanır. Örneğin, çok boyutlu veritabanı (OLAP) veya veri göllerinde (data lake) bulunan verilere analitik SQL uygulanabilir.

SORGU KARMAŞIKLIĞI

SQL, temel sorgu yeteneklerini sağlarken, analitik SQL daha karmaşık sorguları destekler. Analitik SQL, daha gelişmiş analitik fonksiyonlar, pencere fonksiyonları ve analitik ifadeler gibi özelliklerle donatılmıştır. Bu özellikler sayesinde analitik SQL, örneğin veri segmentasyonu, sıralama, sütun bazlı hesaplamalar, koşullu ifadeler ve toplama fonksiyonları gibi analitik işlemleri gerçekleştirmek için daha esnek bir yapı sunar.

İŞLEM AMAÇLARI

SQL, genellikle verilerin saklanması, güncellenmesi, yönetilmesi ve raporlanması gibi veritabanı işlemleri için kullanılır. Bunun yanında, analitik SQL, veri analizi, iş zekası, raporlama, keşif ve tahmin gibi analitik ve istatistiksel amaçlar için kullanılır. Analitik SQL, verilerin içinde gizli olan ilişkileri, desenleri ve eğilimleri keşfetmek için daha özel araçlar ve fonksiyonlar sağlar.

ANALİTİK SQL ÖRNEK SORGU

```
SELECT c.kategori_adı AS kategori,  
       SUM(p.stok_miktarı) AS toplam_satış FROM Ürünler p  
INNER JOIN Kategoriler c ON p.kategori_id = c.kategori_id  
GROUP BY c.kategori_adı  
ORDER BY toplam_satış DESC;
```

Bu sorgu, `Ürünler` tablosundaki ürünleri `Kategoriler` tablosu ile birleştirir (`JOIN`) ve her kategori için toplam satış miktarını hesaplar. Sonuçlar kategori adına göre gruplandırılır (`GROUP BY`) ve toplam satış miktarına göre azalan şekilde sıralanır (`ORDER BY`). Bu sorgu, analitik bir sorgu örneği olarak kategorilere göre satış analizini gerçekleştirir ve en çok satılan kategorileri belirlemeye yardımcı olur.

VERİTABANI YAPISI

ÜRÜNLER (PRODUCTS) TABLOSU:

- `ÜRÜN_ID (PRODUCT_ID)` (BİRİNCİL ANAHTAR)
- `KATEGORI_ID (CATEGORY_ID)`
- `ÜRÜN_ADI (PRODUCT_NAME)`
- `FIYAT (PRICE)`
- `STOK_MIKTARI (STOCK_QUANTITY)`
- `SATIŞ_TARIHI (SALE_DATE)`

KATEGORİLER (CATEGORIES) TABLOSU:

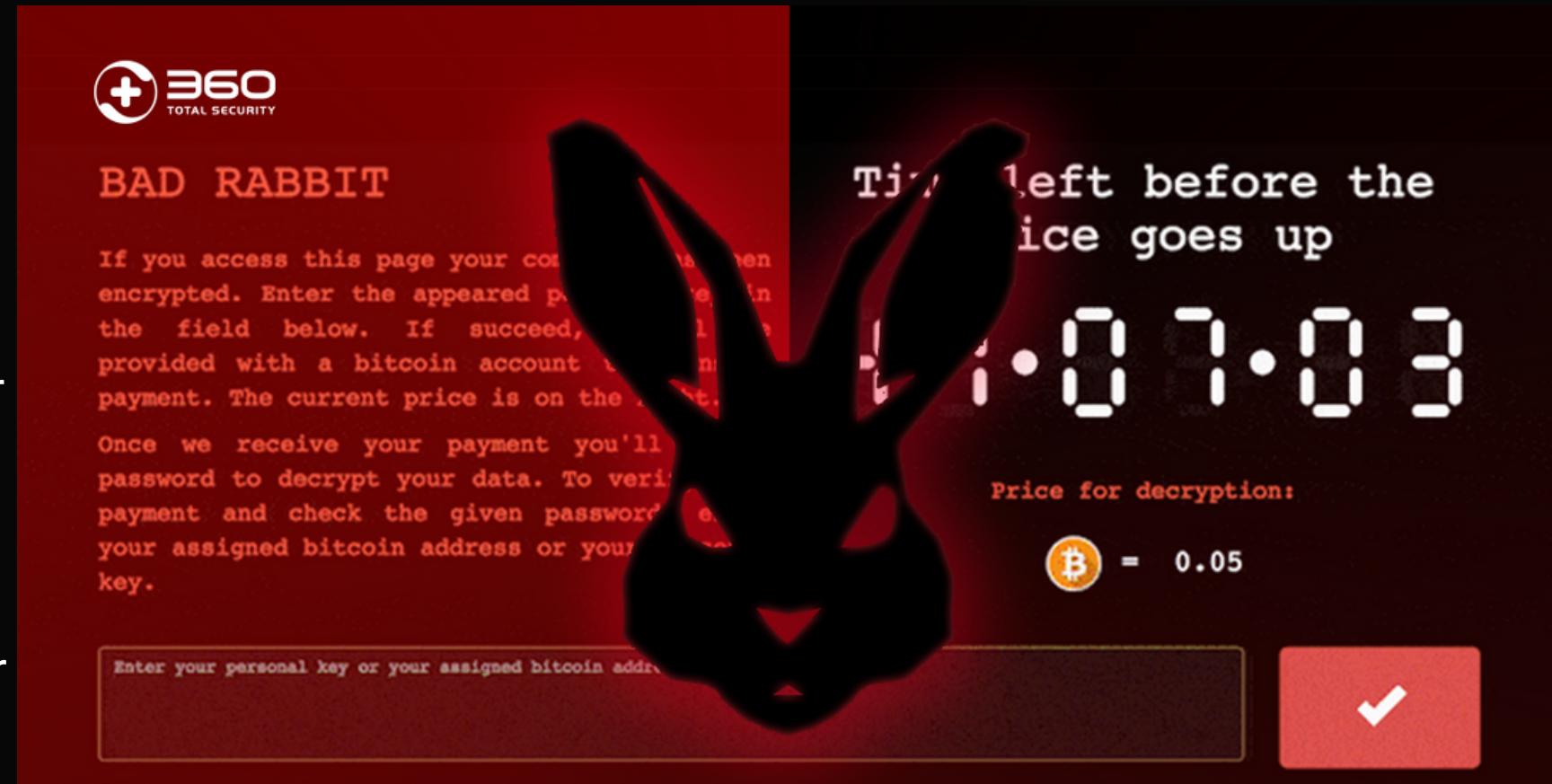
- `KATEGORI_ID (CATEGORY_ID)` (BİRİNCİL ANAHTAR)
- `KATEGORI_ADI (CATEGORY_NAME)`
- `KATEGORI_AÇIKLAMA (CATEGORY_DESCRIPTION)`

BAD RABBIT

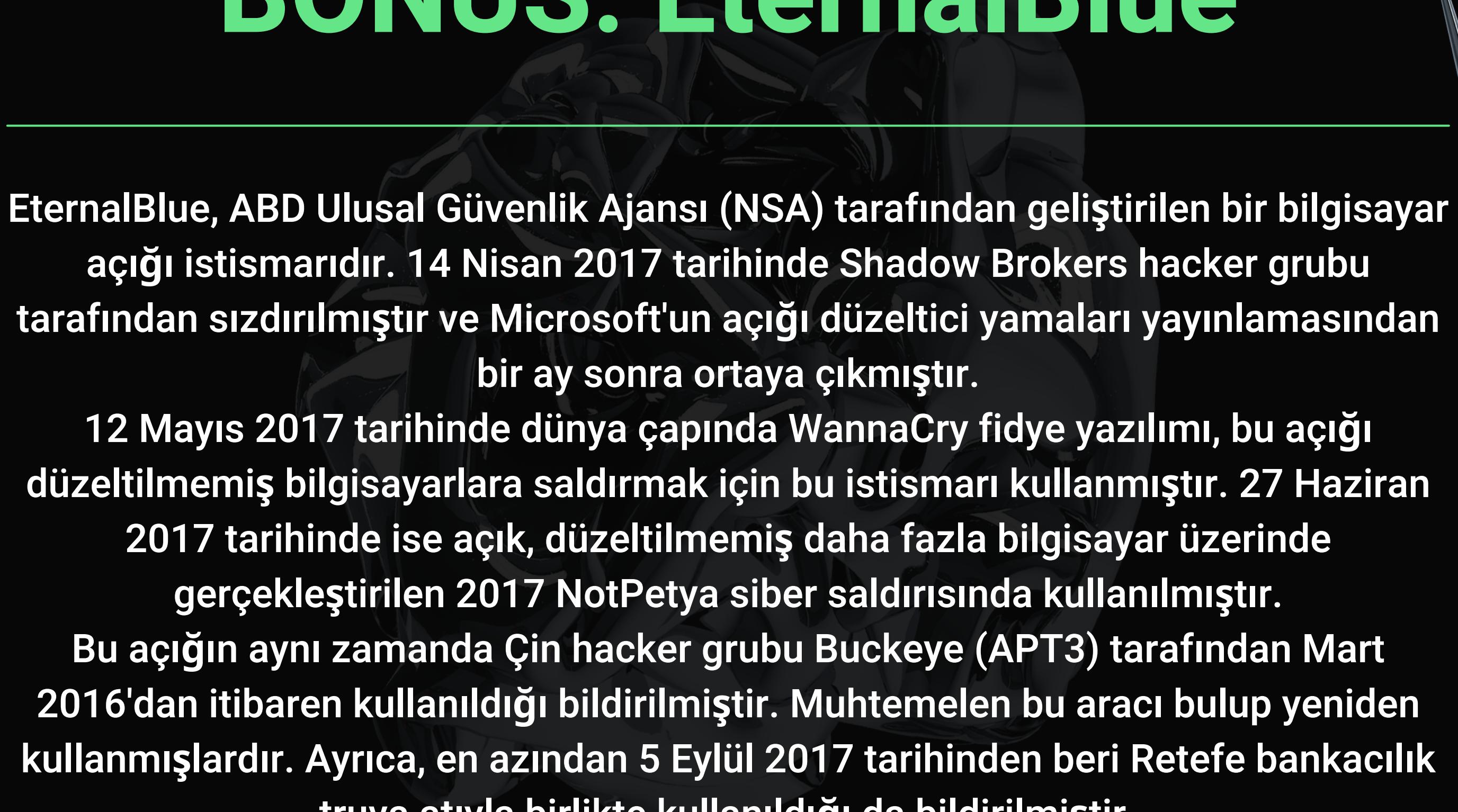
Bad Rabbit fidye virüsü, 2017 yılında ortaya çıkan bir fidye yazılımı saldırısıdır. Bu fidye virüsü, özellikle Rusya ve Ukrayna'da yaygın olarak etkili olmuştur.

Bad Rabbit, kullanıcıların bilgisayarlarına bulaşarak verileri şifreleyen ve bu verilerin kilidini açmak için fidye talep eden bir tür fidye yazılımıdır. Bu saldırı, genellikle kötü niyetli bir web sitesi üzerinden yayılır ve kullanıcılar bu web sitesini ziyaret ettiklerinde kötü amaçlı yazılımı indirirler. Fidye yazılımı indirildikten sonra, bilgisayar kullanıcısı sistemine erişimi kısıtlanır ve fidye notu olarak adlandırılan bir mesajla karşılaşır. Bu not, kullanıcıya verilerinin şifrelendiğini ve dosyalarını geri almak için belirli bir miktarda fidye ödemesi gerektiğini bildirir. Genellikle Bitcoin gibi dijital para birimleriyle fidye ödemesi talep edilir.

Bad Rabbit fidye virüsü, kötü amaçlı yazılımın yayılmasını hızlandırmak için EternalBlue adı verilen bir Windows zayıflığını kullanır. Bu zayıflık, daha önce WannaCry fidye yazılımında da kullanılmıştır.



BONUS: EternalBlue

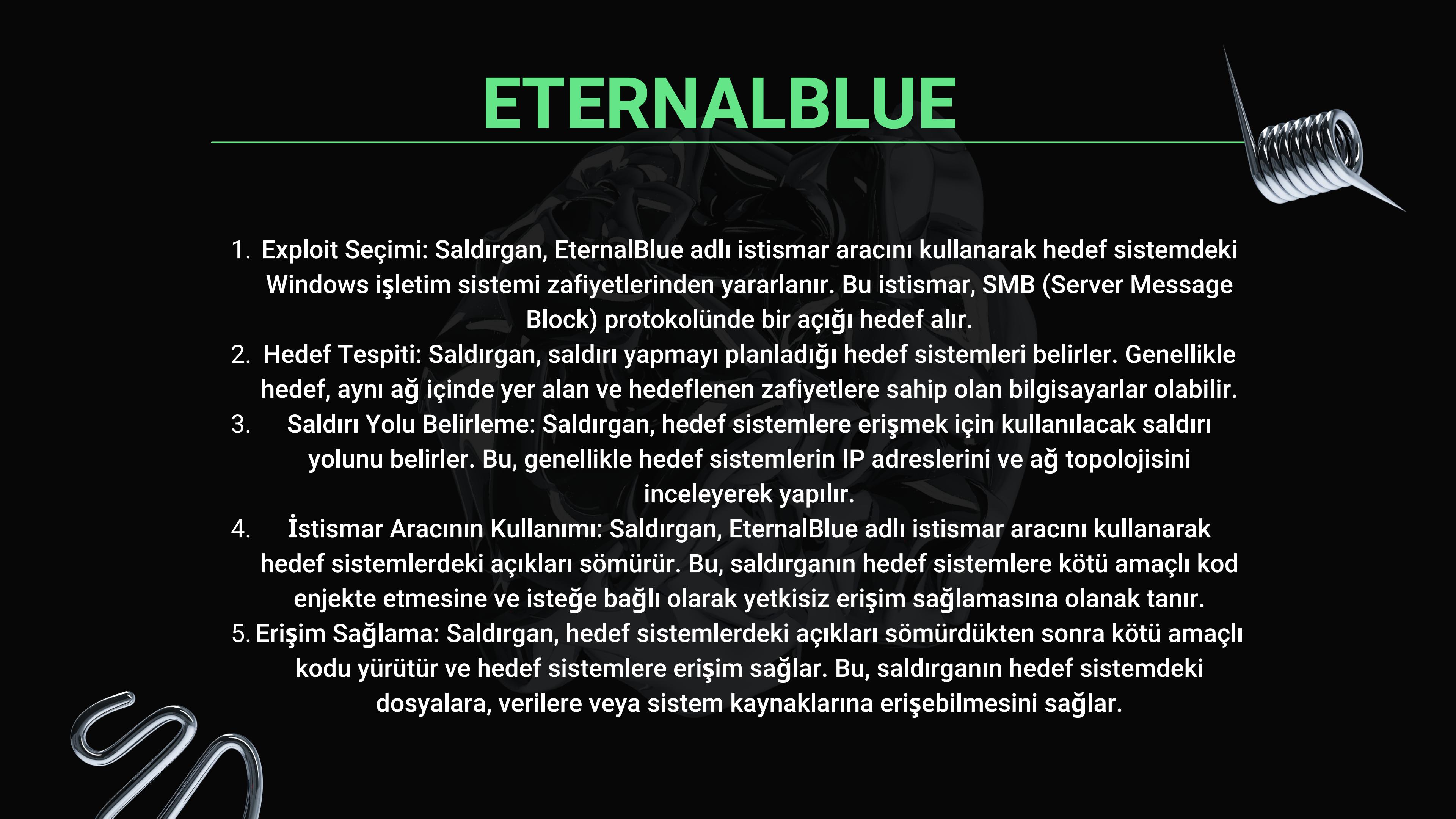


EternalBlue, ABD Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilen bir bilgisayar açığı istismarıdır. 14 Nisan 2017 tarihinde Shadow Brokers hacker grubu tarafından sızdırılmıştır ve Microsoft'un açığı düzeltici yamaları yayınınlamasından bir ay sonra ortaya çıkmıştır.

12 Mayıs 2017 tarihinde dünya çapında WannaCry fidye yazılımı, bu açığı düzeltmemiş bilgisayarlara saldırmak için bu istismarı kullanmıştır. 27 Haziran 2017 tarihinde ise açık, düzeltmemiş daha fazla bilgisayar üzerinde gerçekleştirilen 2017 NotPetya siber saldırısında kullanılmıştır.

Bu açığın aynı zamanda Çin hacker grubu Buckeye (APT3) tarafından Mart 2016'dan itibaren kullanıldığı bildirilmiştir. Muhtemelen bu aracı bulup yeniden kullanmışlardır. Ayrıca, en azından 5 Eylül 2017 tarihinden beri Retefe bankacılık truva atıyla birlikte kullanıldığı da bildirilmiştir.

ETERNALBLUE

- 
1. **Exploit Seçimi:** Saldırgan, EternalBlue adlı istismar aracı kullanarak hedef sistemdeki Windows işletim sistemi zayıflıklarından yararlanır. Bu istismar, SMB (Server Message Block) protokolünde bir açığı hedef alır.
 2. **Hedef Tespiti:** Saldırgan, saldırıyı yapmayı planladığı hedef sistemleri belirler. Genellikle hedef, aynı ağ içinde yer alan ve hedeflenen zayıflere sahip olan bilgisayarlar olabilir.
 3. **Saldırı Yolu Belirleme:** Saldırgan, hedef sistemlere erişmek için kullanılacak saldırının yolunu belirler. Bu, genellikle hedef sistemlerin IP adreslerini ve ağ topolojisini inceleyerek yapılır.
 4. **İstismar Aracının Kullanımı:** Saldırgan, EternalBlue adlı istismar aracı kullanarak hedef sistemlerdeki açıkları sömürür. Bu, saldırının hedef sistemlere kötü amaçlı kod enjekte etmesine ve isteğe bağlı olarak yetkisiz erişim sağlamasına olanak tanır.
 5. **Erişim Sağlama:** Saldırgan, hedef sistemlerdeki açıkları sömürdükten sonra kötü amaçlı kodu yürütür ve hedef sistemlere erişim sağlar. Bu, saldırının hedef sistemdeki dosyalara, verilere veya sistem kaynaklarına erişebilmesini sağlar.

“

Python İle Basit Bir Fidye Yazılımı:

<https://github.com/EymenTakak/PyRansomware>



- *Görev Yöneticisini Engeller.**
- *Sistem Geri Yükleme Yedeklerini Siler.**
- *Sistem Geri Yüklemeyi Kapatır.**
- *Kendisini C ve Windows Dizinlerine Kopyalayıp Başlangıç Dosyası Yapar.**
- *Google Cookielerini Email İle gönderir.**
- *Windows Güncellemelerini Kapatır.**
- *Defenderı Kapatmaya Çalışır.**

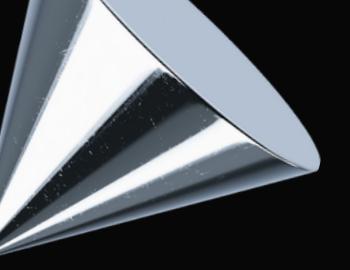
Şifre ALGORİTMASI: SHA256

Şifreyi Tekrarlama Sayısı: 10000

Şifre Uzunluğu: 32

Şifre için salt değer 16 byte boyutunda rastgele bytelar'dan oluşuyor.

Şifrenin ana kısmı 111111-999999 sayıları arasından rastgele olarak seçilir.



Kaynakça

<https://en.wikipedia.org/wiki/EternalBlue>

<https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/>

https://sqlzoo.net/wiki/SQL_Tutorial

<https://medium.com/@gulcanogundur/advanced-sql-fonksiyonlar%C4%B1-window-functions-b0c13c72be39>

