

## UTM DASHBOARD

Projede son düzenlemelerin üzerine öncelikle SuperAdmin kullanıcısının Kullanıcı Listesi sayfasında kullanıcıların son oturum açma tarihlerini görebilmesini sağladık.

Kullanıcı Listesi					
Durum	İsim	Soyisim	Email	Kullanıcı Rolü	Son Giriş Tarihi
	Super	Admin	baris@sau.edu.tr	SuperAdmin	02.06.2023 22:07:04
✓	baris	yilmaz	baris1@sau.edu.tr	Admin	02.06.2023 18:47:47
<a href="#">Yeni Kayıt Oluştur</a>					

Kullanıcının ve SuperAdmin'in yaptığı işlemlerin loglarını tuttuk ve bu logları loglar sayfasında Kullanıcı Logları adında bir tabloda gösterdik. Yöneticinin işlem yaptığı durumlarda ise durum olarak Yönetici badge'i gözükmektedir.

### Kullanıcı Logları

5

kayıt görüntüle

Arama...

Tarih	Kullanıcı	Mesaj	Durum
2023-05-18 01:13:30	baris@sau.edu.tr	Kullanıcı, başarılı giriş yaptı.	Başarılı
2023-05-18 01:19:41	baris@sau.edu.tr	Kullanıcı, hatalı giriş denedi.	Uyarı
2023-05-18 01:19:49	baris@sau.edu.tr	Kullanıcı, başarılı giriş yaptı.	Başarılı
2023-05-18 01:26:30	baris@sau.edu.tr	Kullanıcı, başarılı giriş yaptı.	Başarılı
2023-05-18 01:31:09	baris1@sau.edu.tr	Kullanıcının hesabı oluşturuldu.	Başarılı

52 kayıttan 1 ile 5 arası gösteriliyor

1

2

3

4

5

6

7

...

11

➤

Yalnızca SuperAdmin kullanıcılarının veritabanı indirebilmesi için SuperAdmin paneline Veritabanı İşlemleri sayfası ekledik ve bu sayfada veritabanı yedeğini alabilmektedir. Ayrıca yedeği alan kullanıcıların logları da tutulmakta ve gözükmektedir.

## Veritabanı İşlemleri

### Oluşturan Kişi

### Tarih

baris@sau.edu.tr

18-05-2023 01:19:56

baris@sau.edu.tr

18-05-2023 01:31:39

baris@sau.edu.tr

18-05-2023 01:49:26

baris@sau.edu.tr

02-06-2023 22:14:51

Veritabanı Yedeği İndir

Malware için daha önceden oluşturduğumuz daire grafiğinde logların mesajları görüntülenemediğinden dolayı Malware sayfasına ek olarak kayıtların tablosunu da ekledik.

### Malwares

5 kayıt görüntüle

Arama...

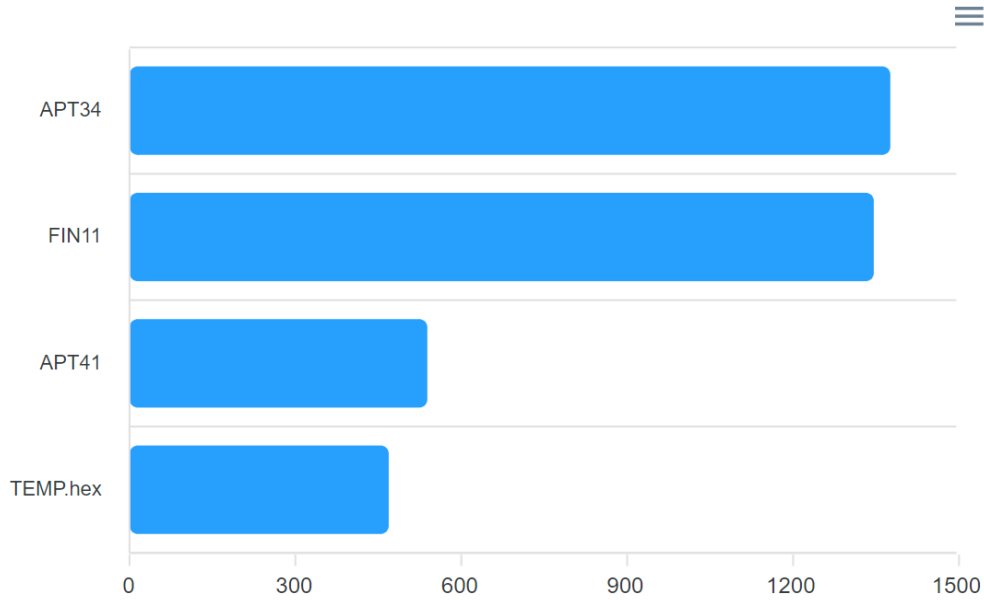
Tarih	Cihaz	Malware Tipi	Mesaj
2022-09-01 00:11:16	7UT85	Rootkit	Sayaç sistemine yerleşen bir rootkit, kullanıcı verilerini çalmaya çalışarak cihazların güvenliğini riske attı.
2023-05-02 03:30:14	6MD85	Worm	Sayaç sistemine bulaşan bir worm, kullanıcı verilerini çalmaya ve kötü amaçlar için kullanmaya çalıştı.
2023-10-26 19:08:28	7UT85	Rootkit	Sayaç sistemine yerleşen bir rootkit, kullanıcı verilerini çalmaya çalışarak cihazların güvenliğini riske attı.
2023-06-05 07:12:51	6MD85	Spyware	Sayaç kullanıcı verilerini toplayan bir spyware, kötü amaçlar için kullanılmak üzere harici bir sunucuya gönderdiği tespit edildi.
2022-09-22 16:55:01	6MD85	Adware	Sayaç kullanıcı arayüzünde istenmeyen reklam içerikleri gösteren bir adware tespit edildi ve kaldırıldı.

399 kayıttan 1 ile 5 arası gösteriliyor

1 2 3 4 5 6 7 ... 80 >

Ayrıca Dashboard'da daha gerçekçi görünmesi açısından Threat Intelligence ve Malware Analysis modüllerini de ekledik. Threat Intelligence sayfasındaki grafikler şu şekildedir:

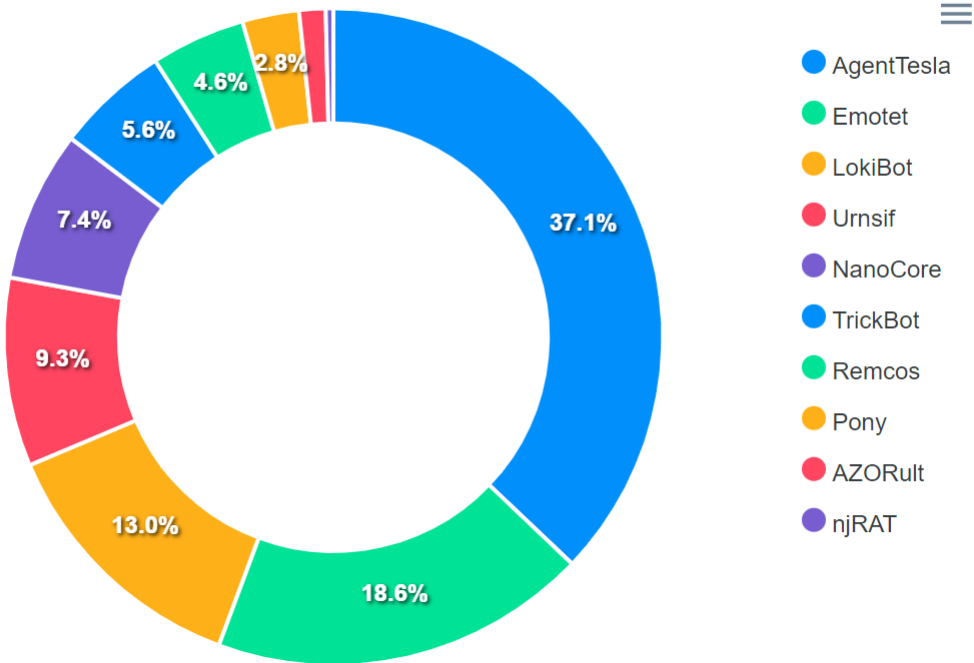
### Actor Activity



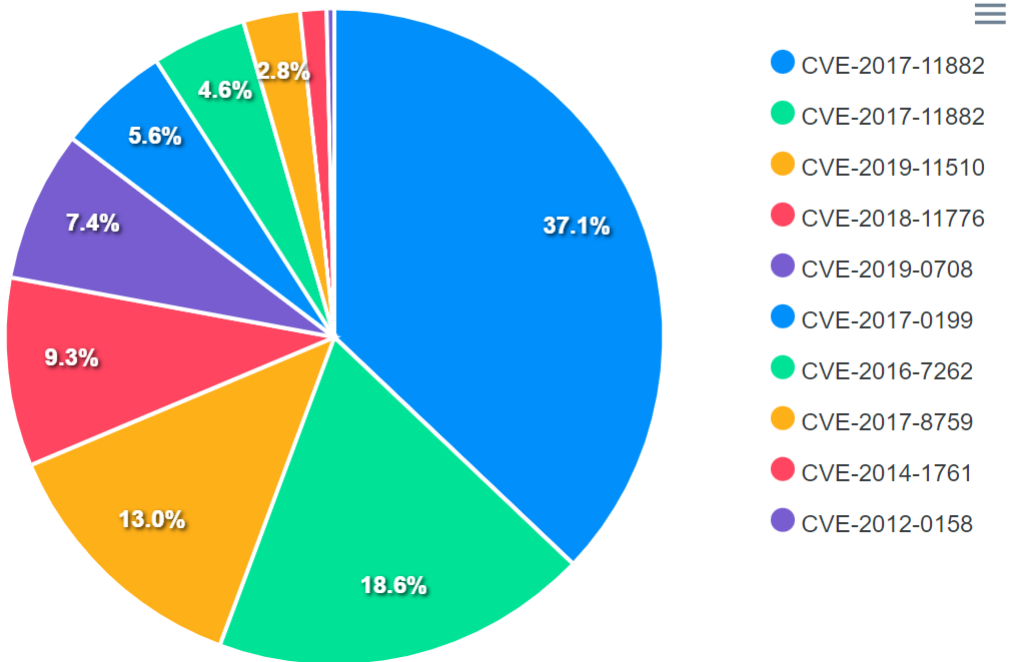
### Recent Activity

- 32 min ● [CVE-2020-14344-x.org libX11 1.6.8 Integer Overflow or Wraparound Vulnerability](#)
- 56 min ● [CVE-2020-6829 - Mozilla NSS 3.54 Use of a Broken or Risky Cryptographic Algorithm Vulnerability](#)
- 2 hrs ● [CVE-2020-12400 - Mozilla NSS 3.54 Use of a Broken or Risky Cryptographic Algorithm Vulnerability](#)
- 1 day ● [CVE-2020-14344-x.org libX11 1.6.8 Integer Overflow or Wraparound Vulnerability](#)
- 2 days ● [CVE-2020-14344-x.org libX11 1.6.8 Integer Overflow or Wraparound Vulnerability](#)
- 4 weeks ● [CVE-2020-14344-x.org libX11 1.6.8 Integer Overflow or Wraparound Vulnerability](#)

Most Active Malware TOP 10



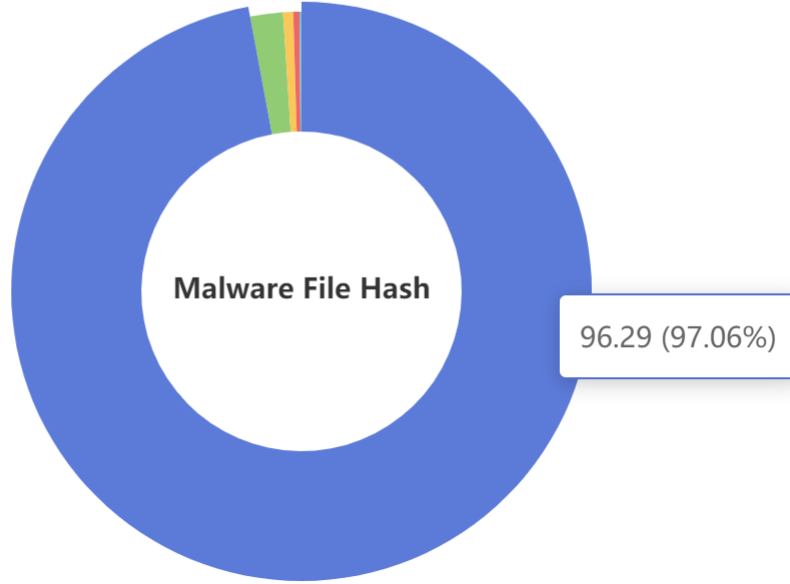
Most Active Vulnerabilities TOP 10



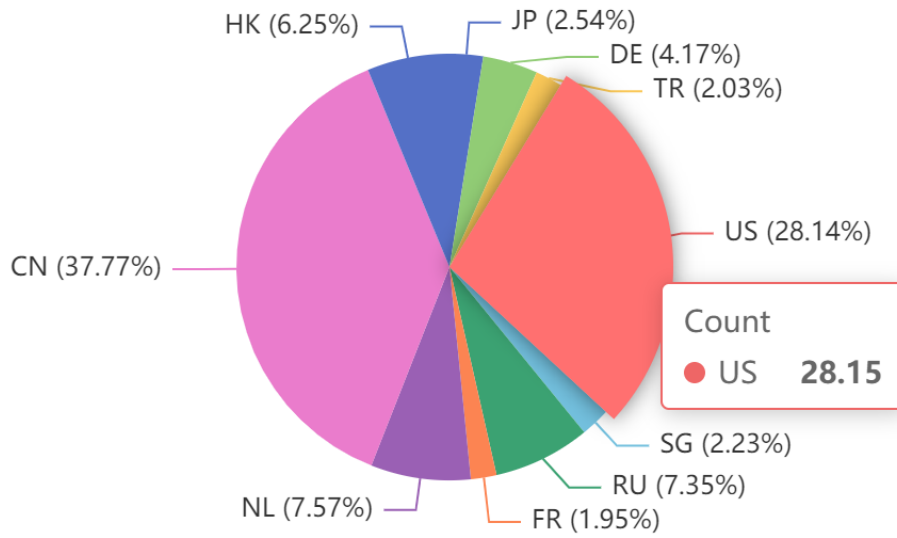
Malware Analysis sayfasındaki grafikler ise şu şekildedir:

## Indicators by iTypes

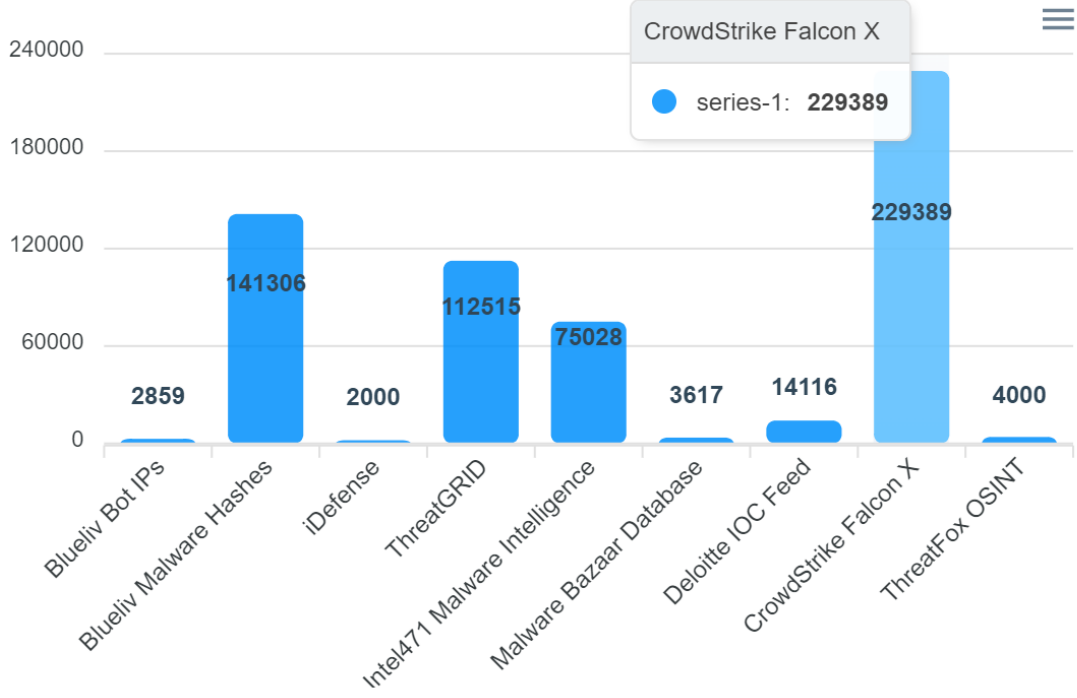
Malware File Hash Malware URL Malware Domain Infected Bot IP  
Malware SSDeep Hash



## Indicators by Origin Country



## Indicators by Source



Ayrıca 2 adımlı doğrulama özelliğini ekledik ve sistemi daha güvenilir hale getirdik. Kullanıcı profilinden kurulum aşağıdaki şekilde görünmektedir:

### Profil

Profil Email Şifre [Two-factor authentication](#)

2 adımlı doğrulamayı etkinleştirmek için aşağıdaki adımları takip edin:

1. Telefonunuza Microsoft Authenticator veya Google Authenticator uygulamasını indirin.
2. Uygulamayı açtıktan sonra aşağıdaki QR Code'u okutun veya bu anahtarı girin: `3rxv hrw5 4ggp q51e 5tpw zaji`  
`ld3t uhxi`



3. Kodu girdiğinizde veya QR'ı okuttuğunuzda uygulama size bir doğrulama kodu vericek. Bu kodu aşağıya girin.

Doğrula

Kurulum yapıldığında ise 5 adet saklanması gereken kurtarma kodu verilmektedir, kullanıcı girişte yalnızca eğer authenticator kurulu cihaza erişimi yoksa bu kodlardan biriyle veya kurulum yapılan uygulamadaki doğrulama koduyla giriş yapabilmektedir. Doğrulama yapılmadığı takdirde giriş mümkün değildir. Kullanıcı kurulumu yaptıktan sonra giriş yaptığımda ise aşağıdaki şekilde doğrulama kodu sorulmaktadır:

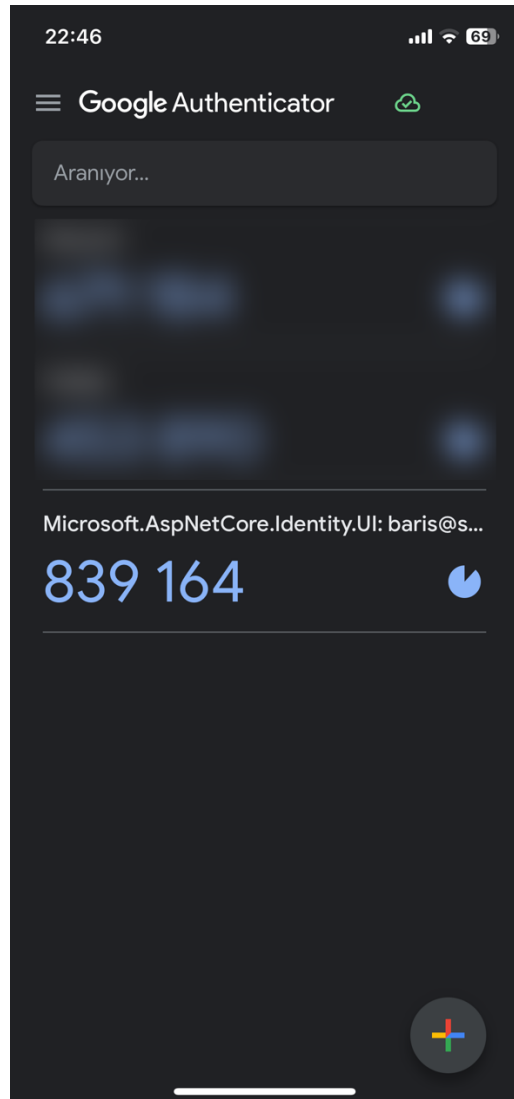
## Two-factor authentication

Authenticator uygulamanızdaki doğrulama kodunu girin.

Giriş Yap

Authenticator cihazına erişiminiz yoksa daha önceden saklamış olduğunuz [kurtarma kodlarıyla giriş yapabilirsiniz..](#)

Örneğin Google Authenticator uygulamasından kurulum yapıldığı varsayılırsa, doğrulama kodu şu şekilde görünmektedir:



Bunlara ek olarak güvenliđi daha da sađlamlařtırmak iin her kullanıcının 2 adımlı dođrulamayı etkinleřtirilmesi zorunlu kılındı ve eđer kullanıcı dođrulamayı etkinleřtirmediyse giriř yaptıđında otomatik olarak 2 adımlı dođrulama kurulum ekranına ynlendirilmektedir ve bu kurulumu yapmadan herhangi bir sayfaya eriřememektedir. Bu iřlemi de bir middleware ekleyerek yaptık. (İřlemleri gerekleřtirmek iin oluřturduđumuz sınıfın ismi “Authenticator2faResourceFilter”)

```
builder.Services.AddMvc(o =>
{
    o.Filters.Add(typeof(ChangePasswordResourceFilter));
    o.Filters.Add(typeof(AuthenticatorResourceFilter2fa));
});
```

Tasarımda hazırlamıř olduđumuz güvenli yazılım geliřtirme ilkelerine ait checkliste ise son rapordan bu yana gelmiř olduđumuz durum ařađıdadır.

- ✓ Yüksek güvenlik gerektiren iřlemlerde tek bir kořula bađlı olarak izin verilmemeli
- ✓ Sistem ve yazılım ierisindeki modller arasında yalıtım sađlanmalı
- ✓ Sunucuda yapılan girdi dođrulama hataları, iřteđin reddi ile sonulanmalı ve iz kaydı oluřturulmalıdır.
- ✓ Yetkisiz bir kullanıcının yazılım ortamından veri alabileceđi, girebileceđi veya yetkisiz iřlemlerde bulunabileceđi noktalar tespit edilmeli, sınırlandırılmalıdır.
- ✓ Kullanılan veritabanının dıřarıya aktarımı ancak veritabanı ynetim yetkisi olan hesaplarla yapılmalı.
- ✓ Hassas iřlevler gerekleřtirilmeden nce, yeniden kimlik dođrulama, daha gl bir mekanizmayla kimlik dođrulama, ikinci faktr veya iřlem imzalama gibi yntemler uygulanmalıdır.
- ✓ Uygulama, bařarısız sistem bařlatma, bařarısız sonlandırma veya bařarısız kapatma gibi iřlemlerde güvenli bir duruma gemelidir.
- ✓ SQL Injection engellemek iin btn veritabanı sorguları, parametre olarak yapılmalı ve veritabanına eriřimde kullanılan dile karřı nleyecek denetimler yapılmalıdır.