umv

WARSS

Website **A**ttack **R**estoration
Security **S**olution

Gerçek zamanlı web sitesi güvenliği

İçindekiler

umv

UMV Inc.

2008 yılında kuruldu

Seoul, South Korea

Web Odaklı Çözümler

Gerçek zamanlı web sunucusu güvenliği

Önlemler

Çalınan veriler, kesintiye uğrayan web hizmetleri,web sitesi tahrifatı, kalıcı saldırılar

Motto

"Bir zincir en zayıf halkasından daha güçlü değildir""

Neden WARSS?

https://www.youtube.com/watch?v=j5rXyhkhvmA

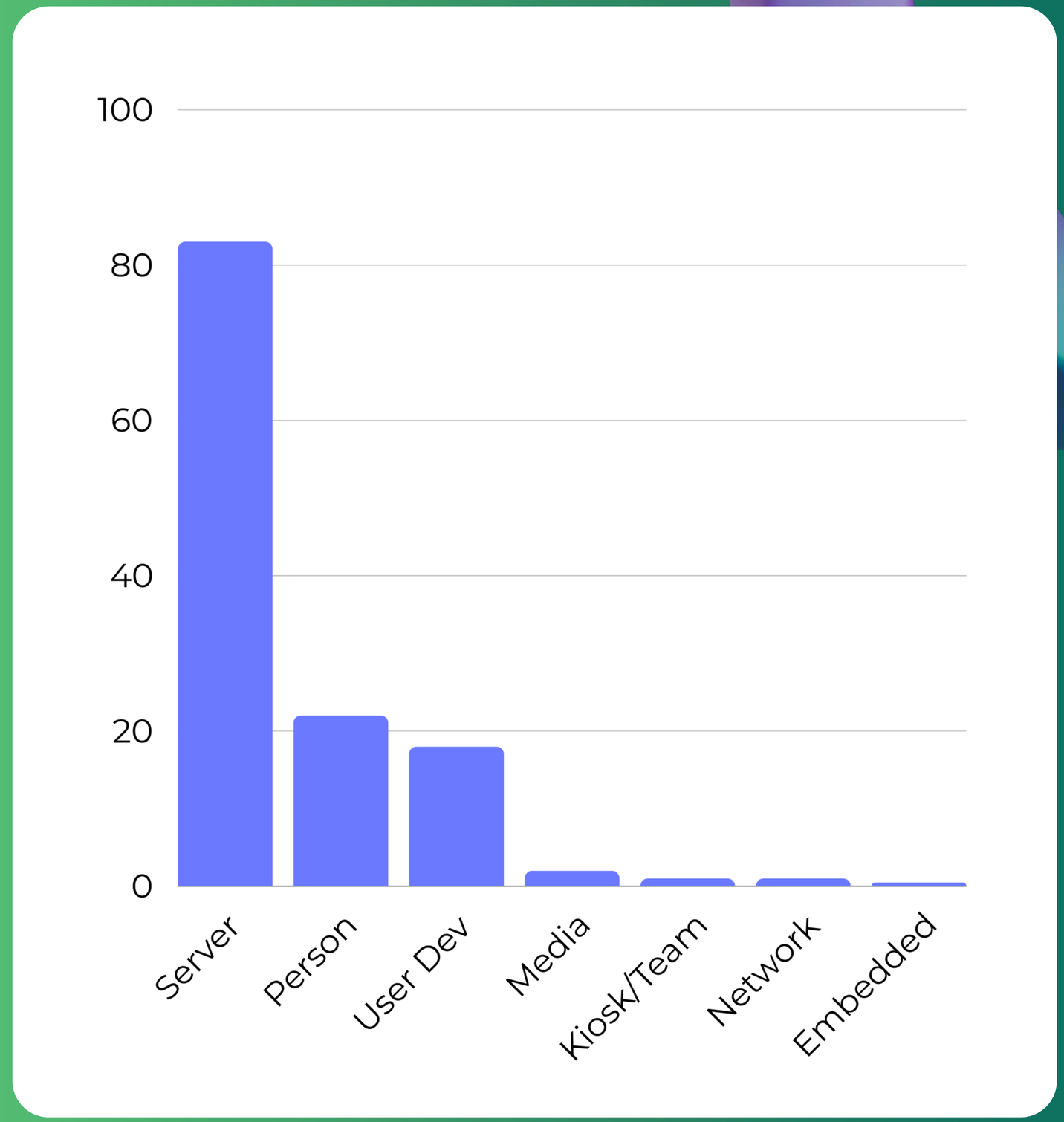
Web Korsanlığı Artışta

Verizon, 2022-2023 yılları arasında doğrulanmış **güvenlik ihlallerinin** sayısında rekor düzeyde **İKİ KAT** artış olacağını analiz etti

2024 Verizon Veri İhlali İnceleme Raporu

İhlallerden Etkilenen Varlıklar

2023 Verizon DBIR



Ukrayna ve Rusya Web Siteleri Saldırıya Uğradı

Yalan Haber

Şubat 2024-Günümüz: Birbirlerine ve müttefiklerine yönelik sürekli siber saldırıların eşlik ettiği Rusya-Ukrayna Savaşı

Yanlış Bilgilendirme ve Veri Toplama

Hedefler arasında KOBİ'ler, medya kuruluşları, devlet kurumları, BT ve kişisel/hassas bilgilere sahip diğer kuruluşlar yer almaktadır

Güvensizlik: Siber Savaşın Anahtarı

Bilgisayar korsanlığı saldırılarının duyurulması siviller arasında korku, yetkililere güvensizlik ve yanlış bilgilendirme yaratır

Image Source: The Record

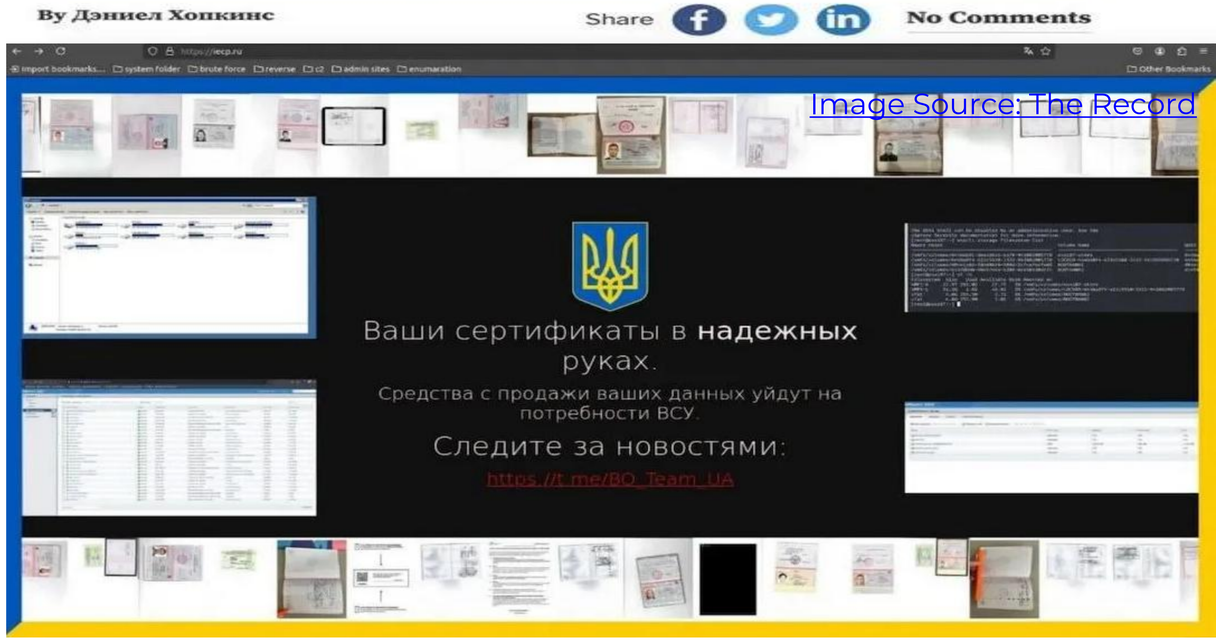


Image Source: The Record

- https://therecord.media/ukrainian-news-outlets-attacked-by-russian-hackers
- https://therecord.media/russia-osnavanie-digital-signatures-cyberattack-ukraine

İnternet Arşivi Saldırıları

1. Tur: DDoS, Sahtecilik, Veri Hırsızlığı

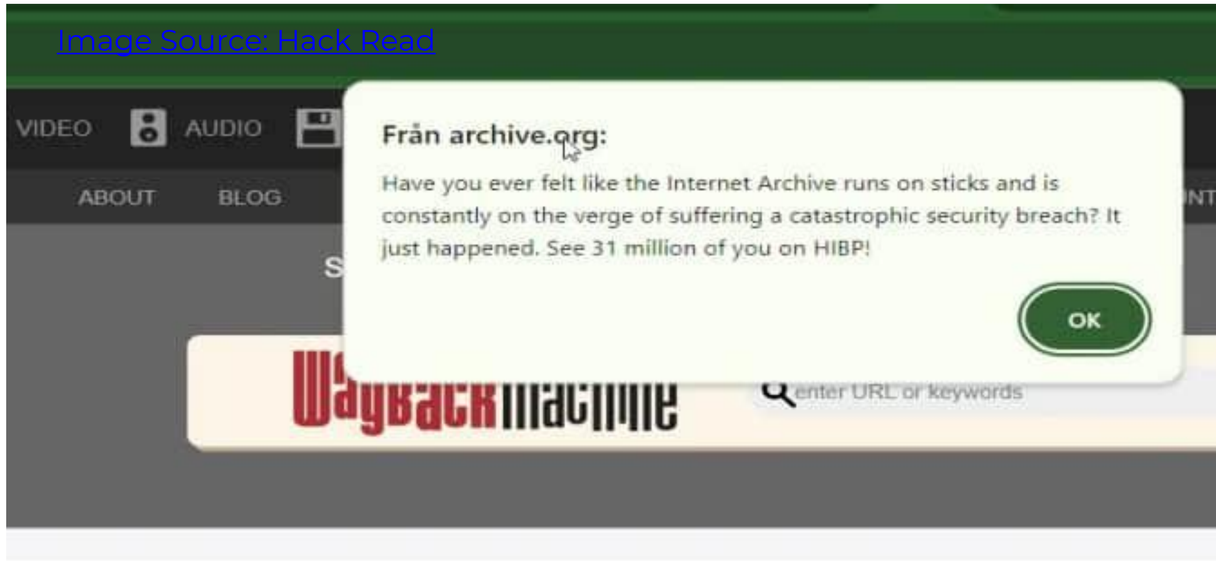
9 Ekim 2024: DDoS saldırısı siteyi çökertti; websitesi **JavaScript** uyarısıyla **tahrip edildi**; **31 million kullanıcı kullanıcı** kullanıcı adları, e-postaları vb. sızdırıldı

Normale Dönüş

18 Ekim 2024: IA verilerin güvende olduğunu ve hizmetlerin geri yüklendiğini onaylar

2. Tur: Güvenli Olmayan Dijital Anahtarlar

20 Ekim 2024: Internet Archive'ın Zendesk destek platformuna erişim sağlamak için döndürülmemiş erişim belirteçlerini istismar etti; **2018**'e kadar uzanan **800** binden fazla **destek biletine** erişti



- https://www.cbc.ca/radio/asithappens/internet-archive-hack-1.7359959
- https://therecord.media/internet-archive-data-breach-ddos-defacement
- https://hackread.com/internet-archive-archive-org-hacked-accounts-compromised/

Trend: Hacktivizm ve Siber Terörizm

- **Siyas**i veya **dini inançları** desteklemek için bilgisayar korsanlığı
- Şifreli iletişim platformlarının (Telegram, Rocket Chat, Discord, vb.) **ve kripto para birimlerinin artan kullanılabilirliği**
  - **TRON** 2021'den bu yana **terör finansmanıyla** ilişkili fonların **%~90**'ını oluşturdu (INTERPOL Yeni Teknolojiler Forumu, Ekim 2023, Merkle Science)
- Hizmet olarak **siber suç** (DDoS, fidye yazılımı, kimlik bilgileri, veriler vb.)

- Yüzeyin Altında Raporu (Haziran, 2024)
  BM Terörle Mücadele Merkezi (UNCCT))

Image Source: Malcontent News

Image Source: POLITICO

- https://unicri.it/sites/default/files/2024-06/DW.pdf

Problemler

Tahrip Etme Yöntemleri

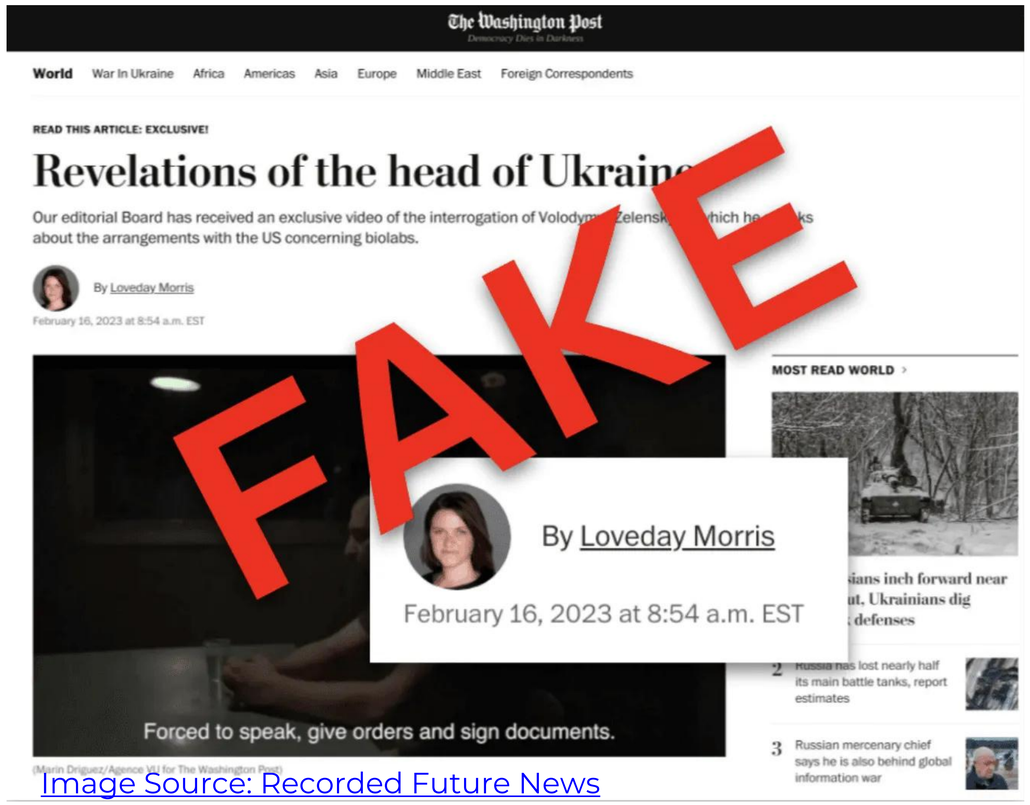
1. **Kaynak Kodunda Değişiklik**

Image Source: alphavilleherald.com

Image Source: boannews.com

Tahrip Etme Yöntemleri

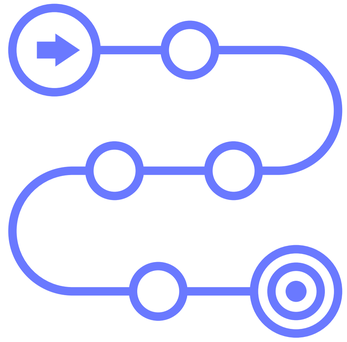
2. İçerik Sahtekarlığı/Enjeksiyonu



[Image Source: Recorded Future News](#)

[Image Source: National Post](#)

Neden Tahrif Ediliyor?



Motivasyon

- hacktivism
- utanç
- şöhret/tanınma
- siber terörizm

Hedef

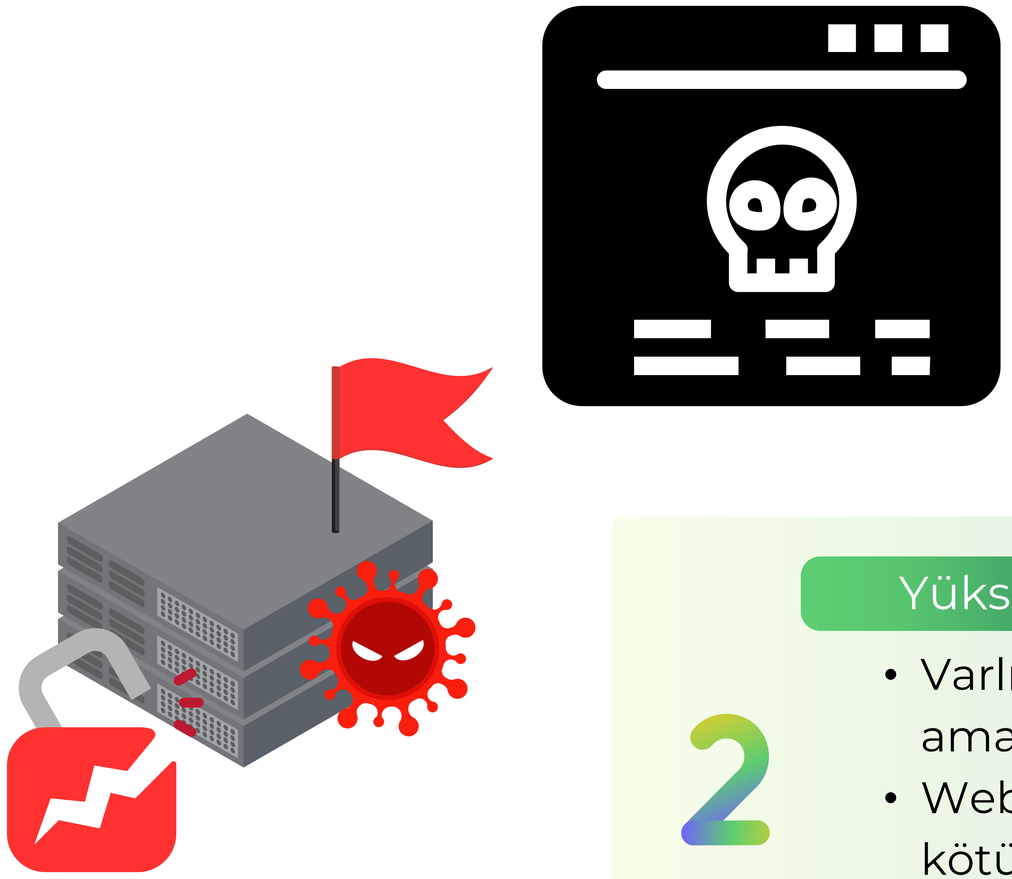
- devlet kurumları
- sağlık hizmetleri
- büyük şirketler
- uygunluk hedefleri

Yöntem

Web tabanlı bileşenlerdeki zayıflıklardan yararlanır:

- web sunucusu
- web uygulamaları
- web siteleri

Bir Web Saldırısının Anatomisi



3 Etki

- Tahrifat
- Kaynak kodu ve içerik sahteciliği

2 Yükselme

- Varlık oluşturmak için web sunucusuna yüklenen kötü amaçlı yazılım
- Web sunucusu dosyalarını değiştirmek için çalıştırılan ek kötü amaçlı yazılım (yük)

1 Sızma

- İlk erişimi elde etmek için kullanılan web sunucusu veya WAS güvenlik açıkları
- Örneğin; SQL enjeksiyonu, çalınan kimlik bilgileri, kimlik avı

Mevcut Durum

Harici Ağ

Şebeke Güvenlik Duvarı

- Ölüm Pingi
- DNS
- FTP
- TELNET
- NetBios

IPS/IDS

- Solucan
- Kural Eşleşmesi

Web Uygulaması Güvenlik Duvarı (WAF)

- SQL enjeksiyonu
- CSRF
- XSS
- Kural Eşleşmesi
- DDoS

Tampon Bölge (DMZ)

Web Sunucusu/WAS

- Bülten tahtası
- Görüntü düzenleyici
- HTTP PUT Yöntemi
- Uzak Dosya Ekleme (RFI)

Dahili Ağ

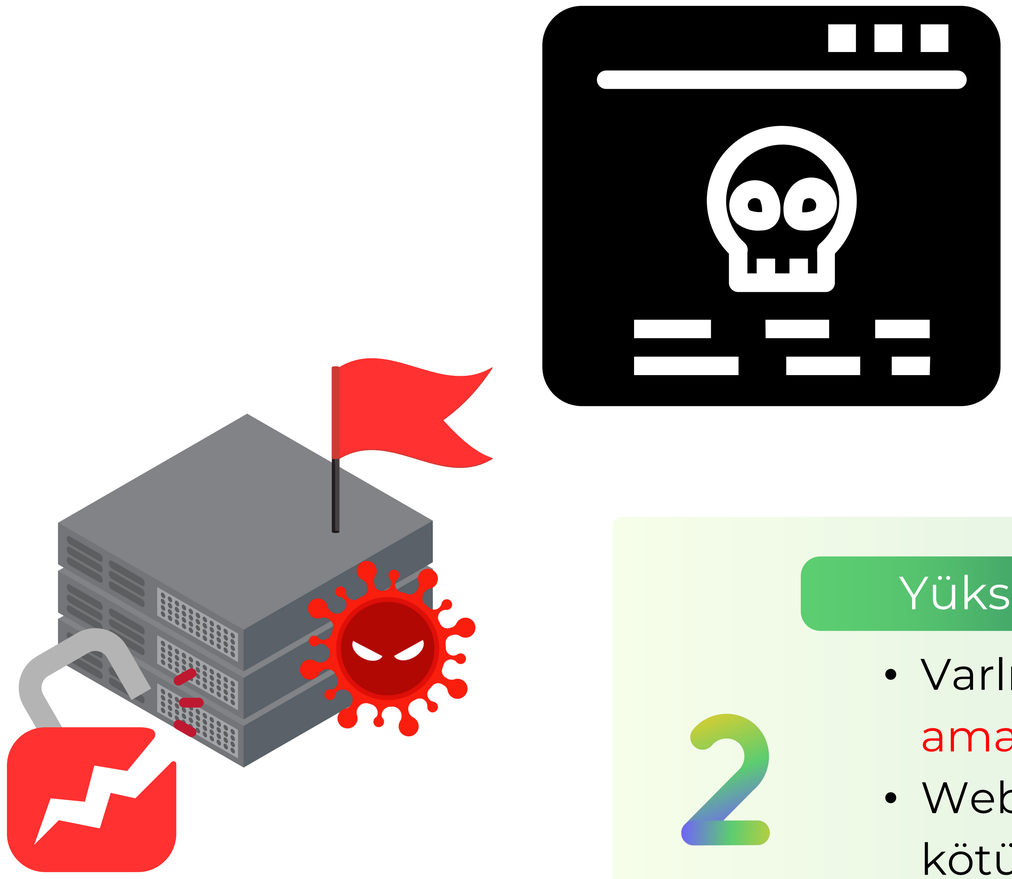
Üretim Sunucu

DTA Sunucuları

- Harici işbirlikçiler
- Dahili çalışanlar

Bağlantı Noktası 80

Bir Web Saldırısının Anatomisi



3 Etki

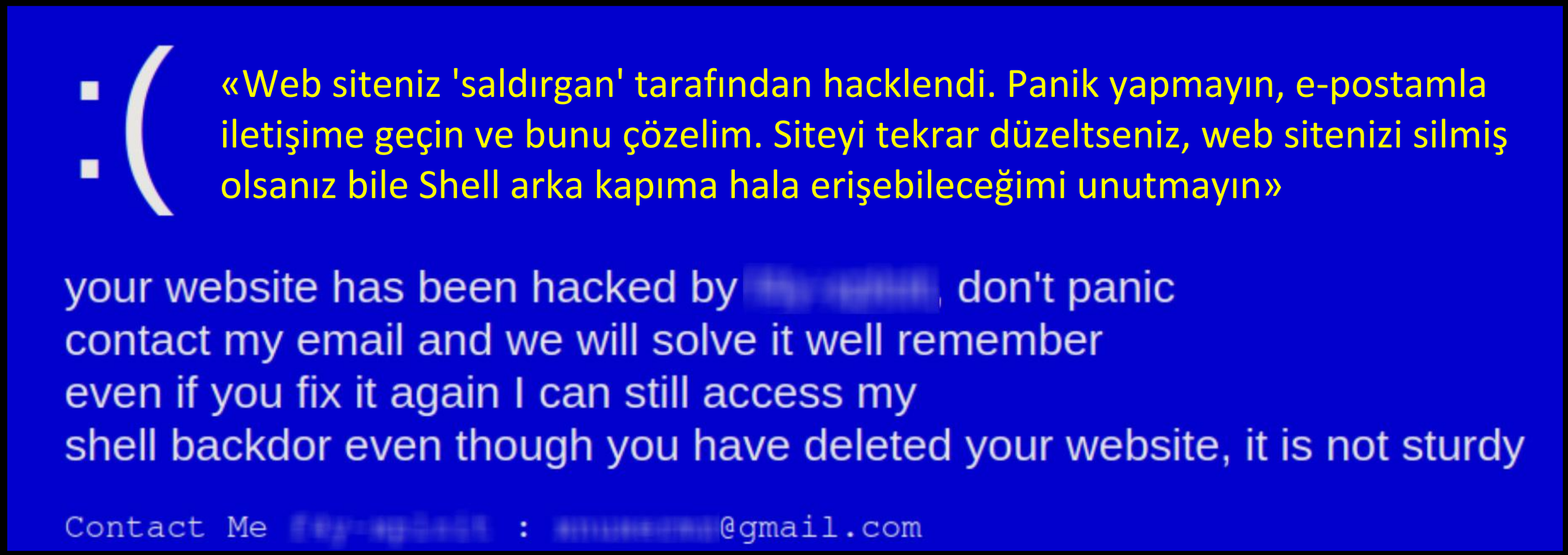
- Tahrifat
- Kaynak kodu ve içerik sahteciliği

2 Yükselme

- Varlık oluşturmak için web sunucusuna yüklenen kötü amaçlı yazılım
- Web sunucusu dosyalarını değiştirmek için çalıştırılan ek kötü amaçlı yazılım (yük)

1 Sızma

- İlk erişimi elde etmek için kullanılan web sunucusu veya WAS güvenlik açıkları
- Örneğin; SQL enjeksiyonu, çalınan kimlik bilgileri, kimlik avı



https://blog.sucuri.net/wp-content/uploads/2023/03/image-1.jpg

Anahtar:
Gerçek Zamanlı Tespit ve Müdahale

Tüm saldırılar üç **değişiklikten** biriyle başlar:

1
Dosya Ekleme

2
Dosya Değişikliği

3
Dosya Kaldırma

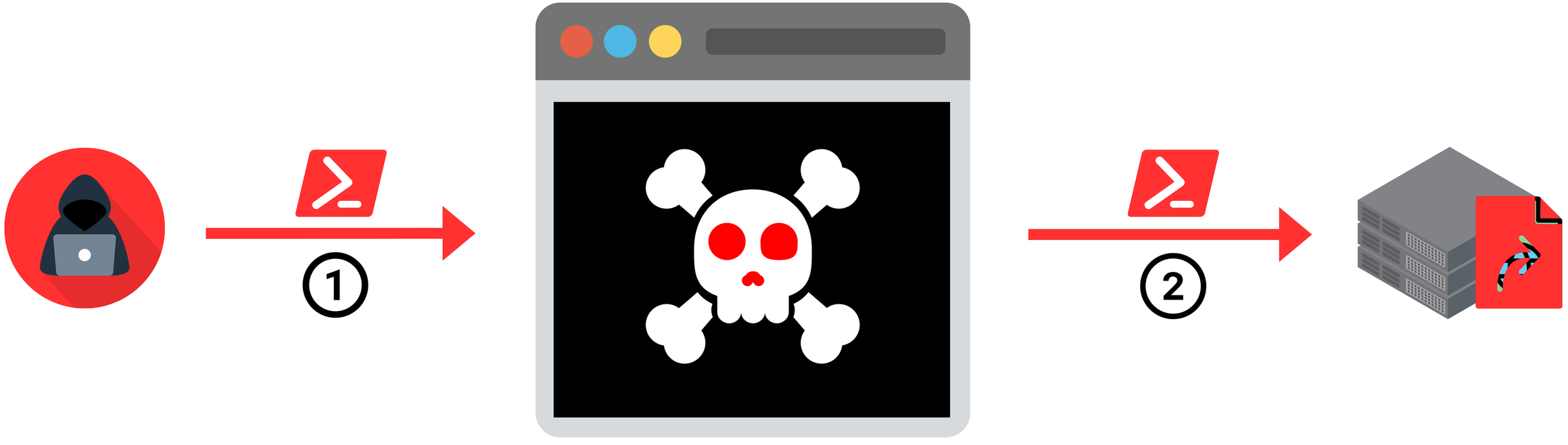
Website **A**ttack **R**estoration & **S**ecurity **S**olution **(WARSS)**

Bir web sitesindeki yetkisiz değişiklikleri **tespit** eden ve orijinal dosyaları **gerçek zamanlı** olarak **geri yükleyen** web sunucusu güvenlik güçlendirici çözümü

Web Sitesi Tahrifatı Nasıl Gerçekleşir?

savunmasız web sitesi

web sunucusu

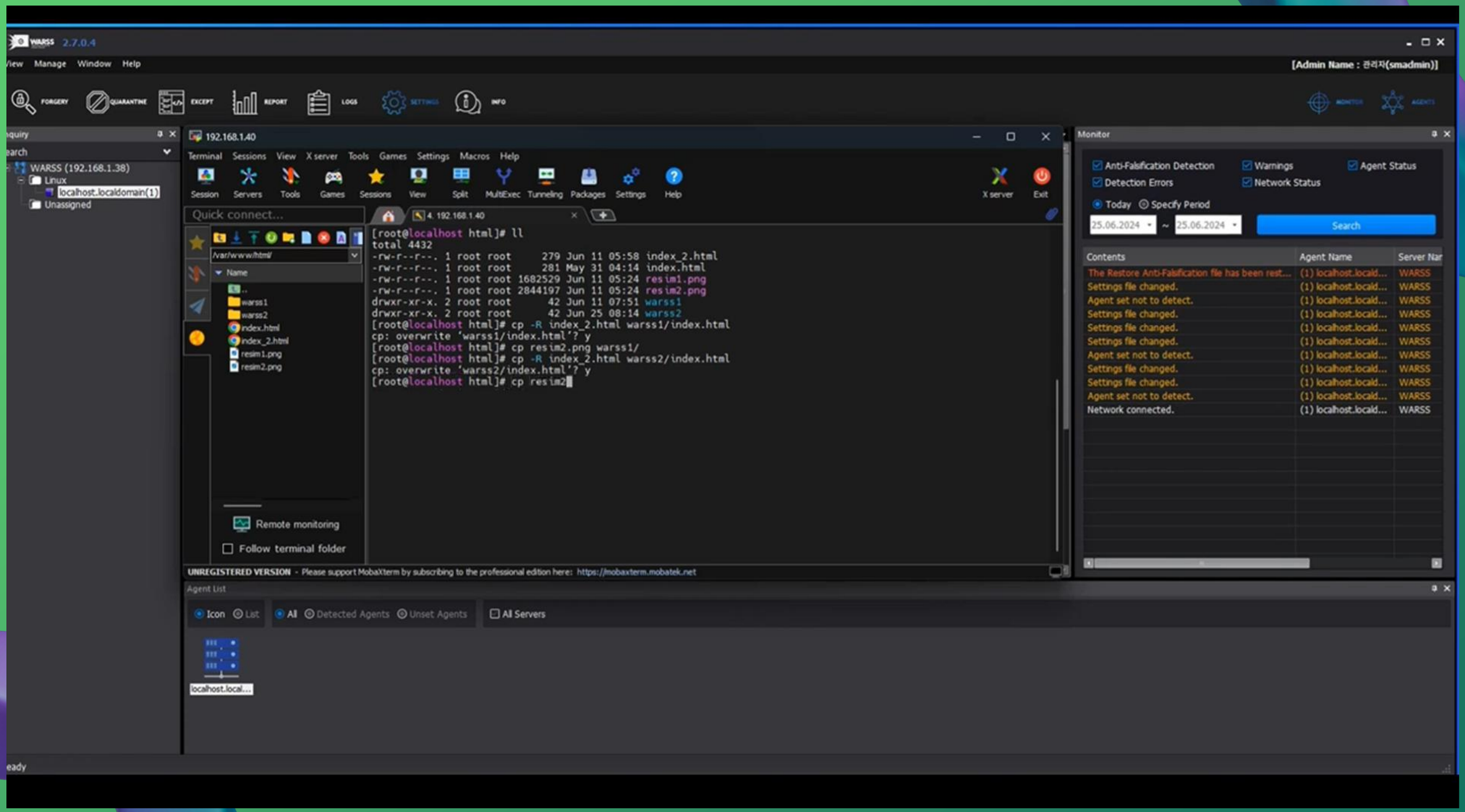


WARSS Nasıl Çalışır?

savunmasız web sitesi

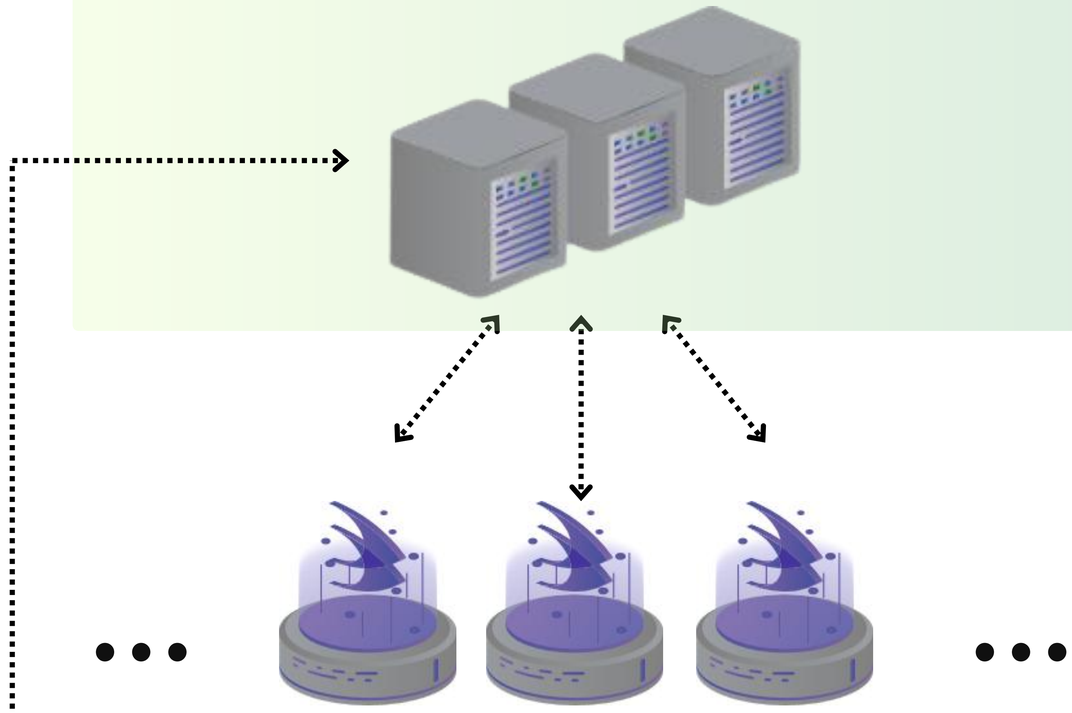
web sunucusu

Demo



https://www.youtube.com/watch?v=B20LDk0iAJQ

WARSS Yapılandırması

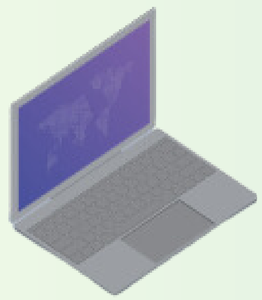


WARSS Yönetim Sunucu(ları)

- HW/VM üzerinde kurulu sunucu yazılımı
- Temsilcileri uzaktan yönetir ve kontrol eder
- Algılama geçmişini kaydeder
- Güncellemeleri ve ayar değişikliklerini Temsilcilere dağıtır

WARSS Temsilci(ler)i

- Web sunucusu/WAS üzerinde yüklü program
- Dosya değişikliklerini algılar
- Unix, Linux, Windows NT O/S ile uyumludur
  (JDK 1.5+'yı desteklemelidir)



WARSS Yönetici Programı

- Yönetici bilgisayarında yüklü program
- Şunlar için ayarları kontrol eder: algılama, uzaktan eylem, ortam ve raporlama
- Yönetim, istatistik ve raporlama ayarlarına erişim

WARSS Nasıl Farklıdır?

	WARSS	Web Crawlers
		
Tespit Yöntemi :	**Gerçek zamanlı**, model tabanlı	**Periyodik** algılama
Yükleme :	**Optimize** edilmiş kaynak kullanımı **(~%1 CPU)**	**Ajansız**
Hedef Tespit:	**Sunucu dosyaları** (kaynak kodu, veriler, içerikler)	**Derlenmiş URL birimleri ve veri dosyaları**
Etki azaltma:	**Gerçek zamanlı, otomatik** restorasyon	İhlal üzerine **manuel hafifletme**

Gerçek zamanlı algılama

Kaynak kodunu ve içeriğini koruma

Hafif Ağırlık

Anında restorasyon ve iyileşme

SIFIR GÜVEN

1. “Asla güvenmeyin, her zaman doğrulayın”

2. En az ayrıcalıklı erişim

3. İhlal olduğunu varsayayalım

SIFIR GÜVEN

3. İhlal olduğunu varsayalım

Gerçek zamanlı algılama

Gerçek zamanlı dosya değişikliği izleme

Kolaylaştırılmış yönetim

Gerçek zamanlı uyarılar ve raporlar

Hızlı hafifletme

Otomatik restorasyon ve kurtarma

Uygunluk

bilgiye ihtiyaç duyulduğunda erişilebilir

ISO/IEC 27001 Prensipleri

Gizlilik

sadece yetkili tarafların erişebildiği bilgiler

Bütünlük

bilgilerin doğru olması ve yolsuzluktan korunması

ISO/IEC 27001 Uyumluluk

Uygulanabilir Gereksinimler :

8.1 Operasyonel planlama ve kontrol

8.3 Bilgi güvenliği risk tedavisi

9.1 İzleme, ölçme, analiz ve değerlendirme

ISO/IEC 27001 Uyumluluk

Uygulanabilir Ek A Teknolojik Kontroller:

8.4 Kaynak koda erişim
8.6 Kapasite yönetimi
8.7 Kötü amaçlı yazılımlara karşı koruma
8.8 Teknik güvenlik açıklarının yönetimi
8.12 Veri sızıntısını önleme
8.13 Bilgi yedekleme
8.15 Günlük kaydı
8.16 İzleme faaliyetleri
8.23 Web filtreleme
8.26 Uygulama güvenliği gereksinimleri

GS (Good Software) (İyi Yazılım) Seviye 1 Sertifikalı

- **Test Standartları:**
  ISO/IEC 25023, 25051, 2504
- **Şunun için test edilmiştir:**
  - İşlevsel uygunluk
  - Performans verimliliği
  - UyumlulukKullanılabilirlik
  - Güvenilirlik
  - Güvenlik
  - Bakım
  - Taşınabilirlik

Kullanım Örnekleri

Devlet Savunma Kurumu

Güvenlik Eksiklikleri

“W” web tabanlı sahtecilik tespit yazılımının performansından ve yönetim kolaylığından memnun değil

Onların Kontrol Listesi

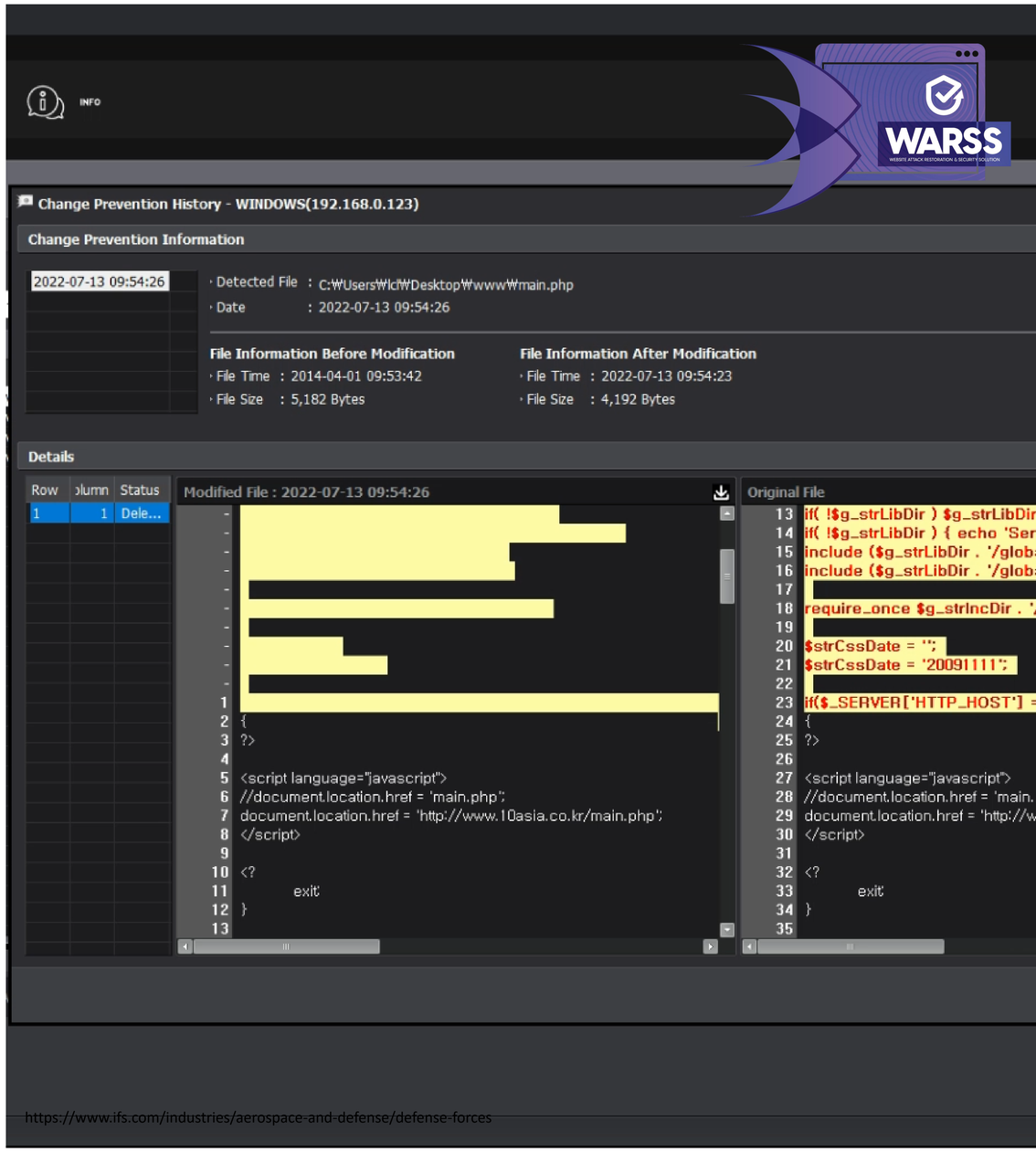
Özellikle otomatik restorasyon ve verimli yönetim sunan Ajan tabanlı bir çözüm arıyorduk

2023 WARSS Uygulaması

Tüm web sunucularına 50 WARSS Ajanı yüklendi

Onların Geri Bildirimi

WARSS'ın URL'leri manuel olarak girmeden kolay algılama yapılandırmasına olanak tanıyan otomatik ana dizin algılama özelliğinden memnunuz



https://www.ifs.com/industries/aerospace-and-defense/defense-forces

Ulaştırma Ajansı

İçerik Sahteciliği Endişeleri

Eğitim içerikli (resimler, videolar) web sitesi işletmek; tescilli sahteciliğe karşı çözümün geliştirilmesinde dış kaynak kullanımını denendi ve başarısız olundu

Neden WARSS?

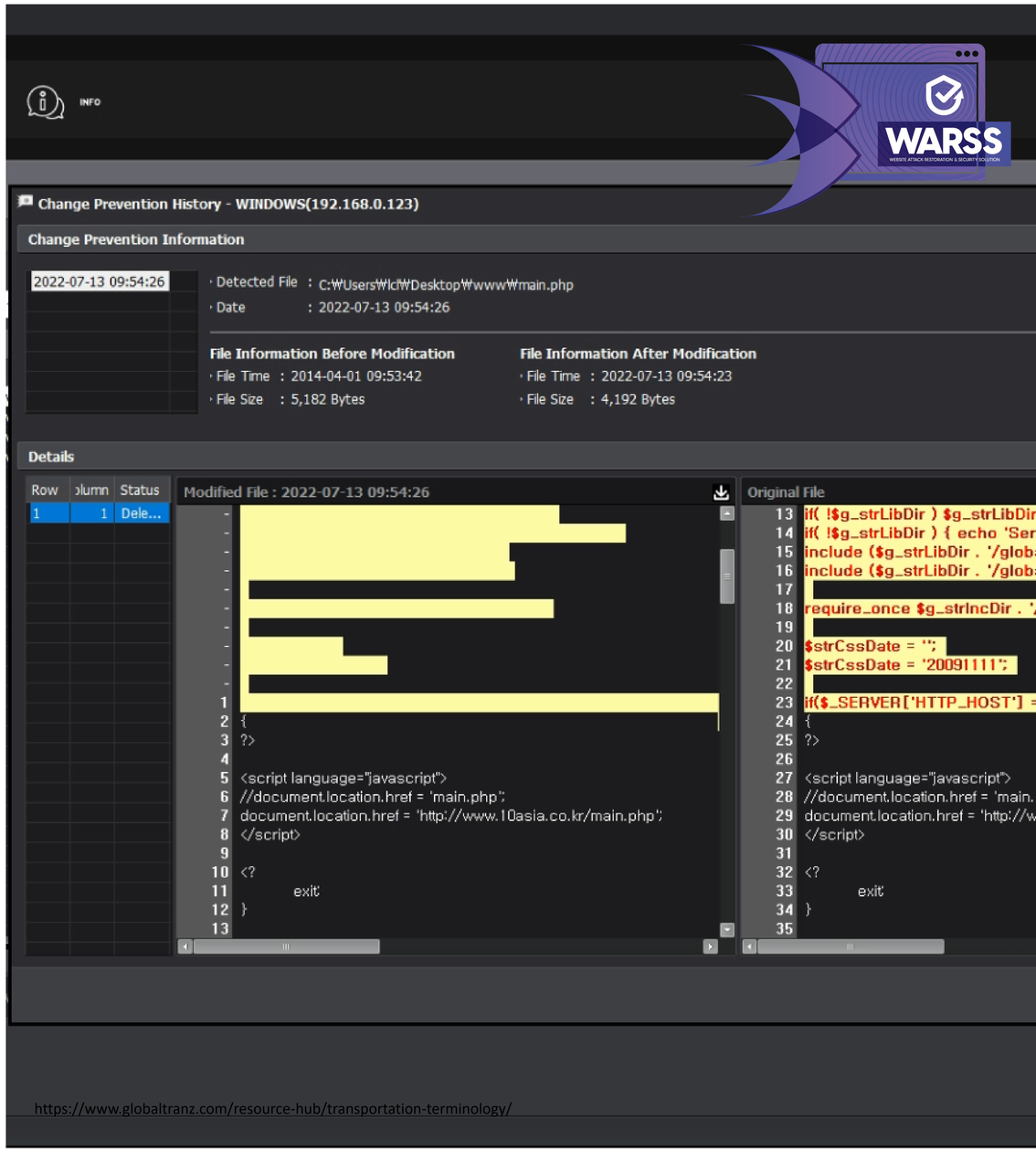
Test ettikleri diğer tüm sahtecilik karşıtı çözümlerle karşılaştırıldığında, WARSS kaynak kodu, görüntü ve video sahteciliğine karşı koruma sağlayan tek çözümdü

Neden WARSS'ı Seçtiler

Tüm web sunucularına 100 WARSS Ajanı yüklendi

Sürekli Koruma

WARSS o zamandan beri herhangi bir sahtecilik olayını önledi; müşteri, sistemlerine her sunucu eklediğinde Ajan satın almaya devam eder



https://www.globaltranz.com/resource-hub/transportation-terminology/

WARSS'ı Kimler Kullanıyor?

WARSS birçok ulusal şirket ve kurumun itibarını korumaktadır.

대 한 민 국
청 와 대

대한민국육군
Republic of Korea Army

한국지역난방공사
KOREA DISTRICT HEATING CORP.

국 방 과 학 연 구 소
Agency for Defense Development

ETRI
한 국 전 자 통 신 연 구 원
Electronics and Telecommunications Research Institute

서울특별시
SEOUL METROPOLITAN GOVERNMENT

영남대학교
Yeungnam University

LS ELECTRIC

한전원자력연료
KEPCO NUCLEAR FUEL

... and more!

Yüzlerce Müşteri

UMV ürünleri, on yılı aşkın bir süredir yüzlerce müşterinin web sunucusu için güvenli ve istikrarlı koruma sağlamaktadır.

SAMSUNG
13+ years

amazon web services
13+

ebay
7-8

Hanwha
13+

NongHyup Bank
10+

Prudential
13+

TOYOTA

STARBUCKS

dun & bradstreet

SUPREME COURT OF KOREA

Seoul Metro

S-OIL Corporation

Ministry of National Defense
Republic of Korea

OFFICE OF THE PRESIDENT
THE REPUBLIC OF KOREA

HYUNDAI

Deloitte.

iMBC

... ve çok daha fazlası!

Teşekkürler

Bize Ulaşın

UMV Inc.

Seoul, South Korea

+82 2 448-3435

sales@umvglobal.com

www.umvglobal.com

UMV Yazılım

İstanbul, Türkiye

+90 212 266 21 88

sales@umvglobal.com

www.umvglobal.com

Ek Bilgiler

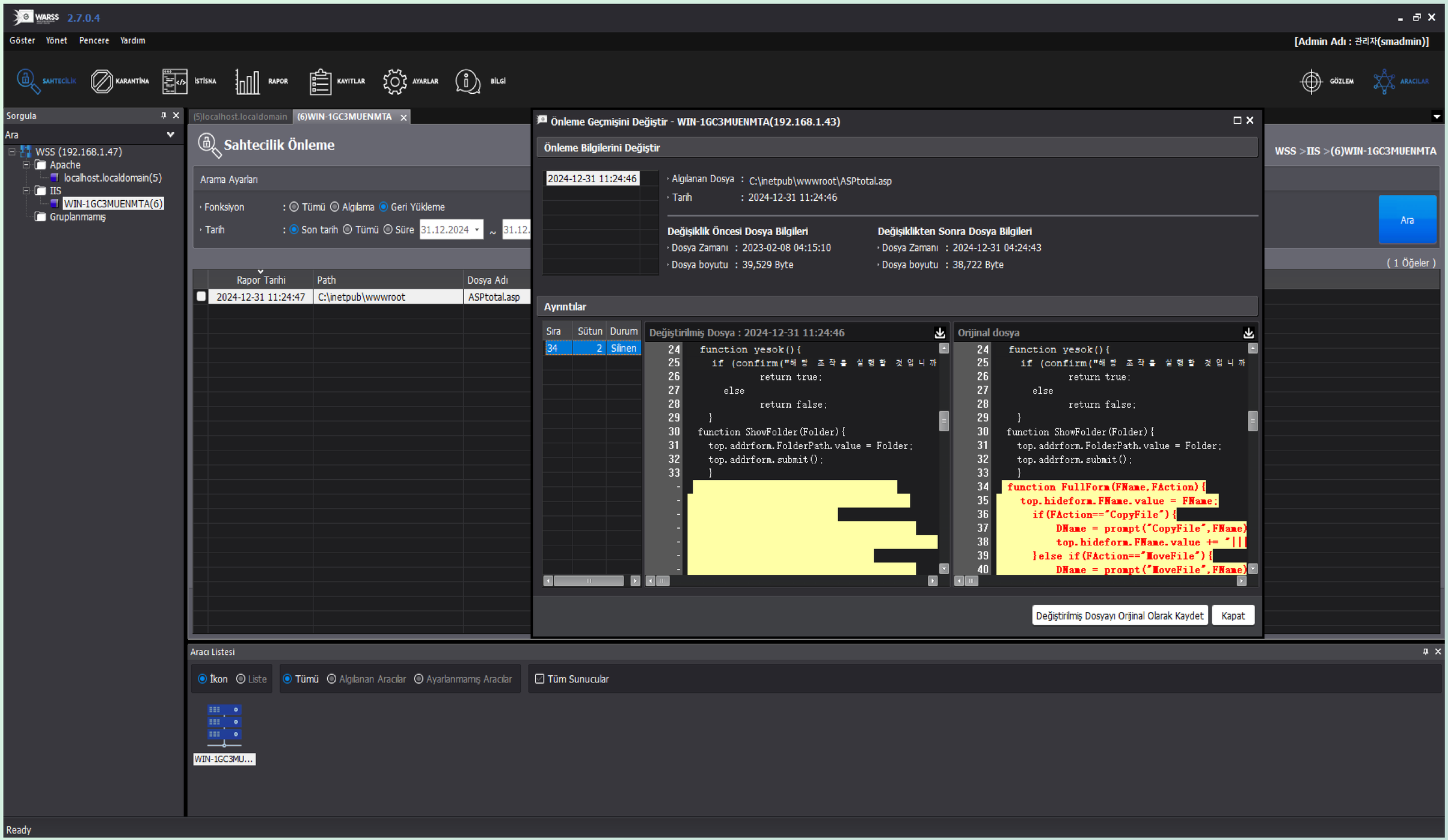
WARSS İşlevleri

Sahtecilik Tespiti ve Restorasyonu

İşlev Adı	Açıklama
Sahtecilik Tespiti	Web sitesi kaynak dosyalarının ve verilerinin sahteciliğinin ve değiştirilmesinin tespiti ve bildirimi
Sahtecilik Restorasyonu	Sahtecilik tespit edildiğinde orijinal dosyaların gerçek zamanlı olarak geri yüklenmesi
Orijinali Yeniden Atama	Meşru değişiklikler yapılması gerektiğinde temel/orijinal dosyaları yeniden atayın

Sahtecilik Tespit Görünümü

Sahtecilik Tespiti ve Gerçek Zamanlı Restorasyon



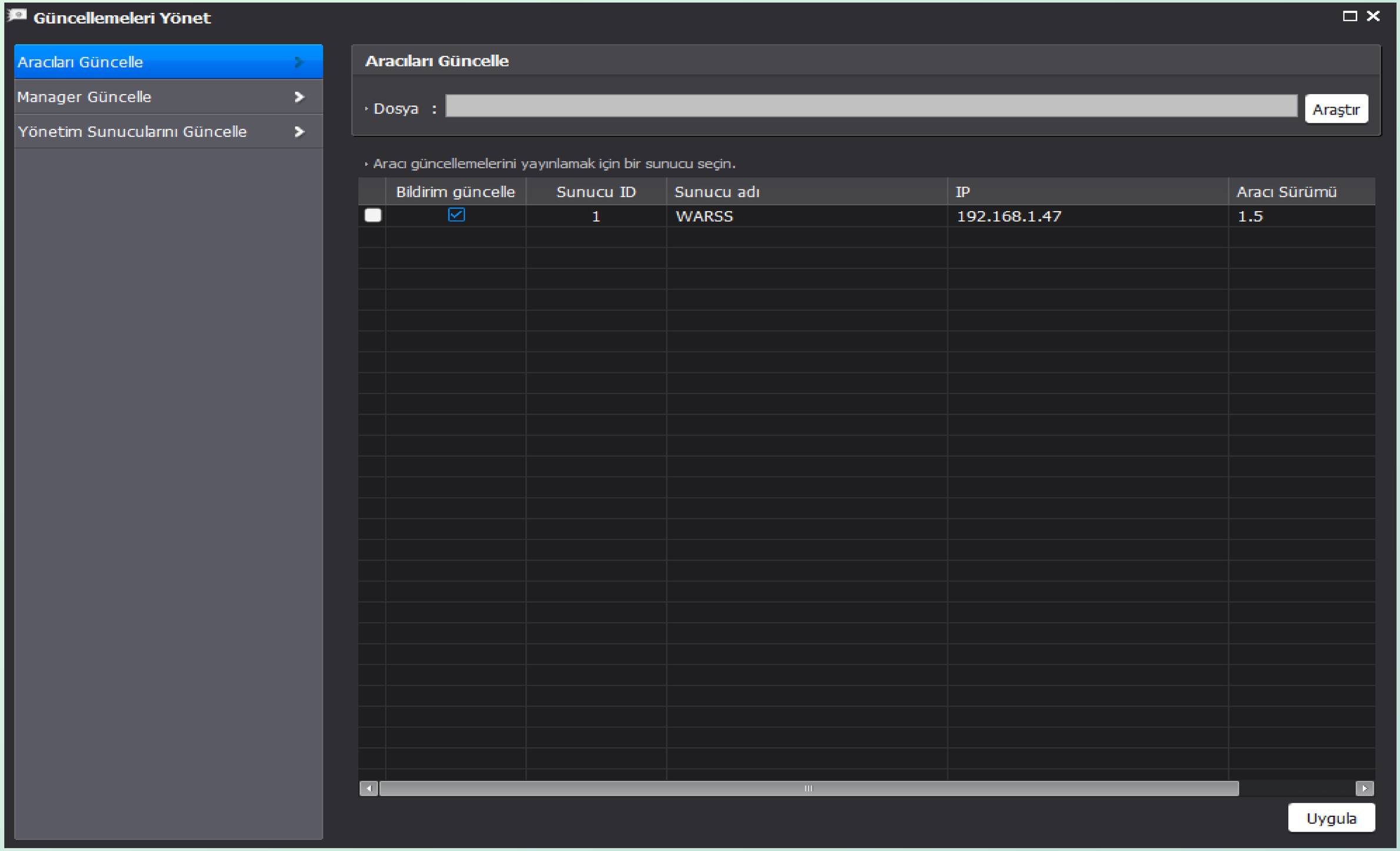
WARSS İşlevleri

Yönetim Özellikleri

İşlev Adı	Açıklama
Güncelleme Yönetimi	Temsilci ve Yönetici güncellemeleri, sürüm yönetimi
İzinler ve Raporlama Yönetimi	• Hesap ve kullanıcıya göre izin yönetimi • Harici sistemlerle arayüz oluşturma (ESM, SMS, E-posta, vb.) • Raporlar ve istatistikler
İstikrar	• Kaynak kullanım kontrolü • Sunucu ortamına uygun özelleştirmeler
Saldırgan IP Tespiti	Sahte dosyalar için yürütme IP raporları (yalnızca algılama işlevi etkinleştirildiğinde kullanılabilir)
Tercih Yönetimi	Web/WAS yapılandırma dosyası yönetimi ve değişiklik algılama ayarları
Özel Güvenli Yükleyici	• Her kullanıcı hesabı için güvenli yükleme hedef dizinini belirtin • Güvenli Yükleyici kullanılarak yüklenen dosyalarda kötü amaçlı kod olup olmadığını da kontrol edin

Yönetim Görünümü

Güncelleme Yönetimi



Yönetim Görünümü

Yönetici İzinleri

Yönetim Görünümü

İstikrar

Ayarlar

WARSS >IIS >(6)WIN-1GC3MUENMTA

Genel | WAS | Dosya Algılama | Gelişmiş

Sunucu Erişim Ayarları

Genel

WSS Sunucu Adresi 1	: 192.168.1.47	Öncelikli Erişim	Port : 7778	İyileşme süresi : 0 saniye			
WSS Sunucu Adresi 2	: 127.0.0.1	Öncelikli Erişim	Port : 7778				
Sunucu Adresini Yükle	: 192.168.1.43		Port : 7777				
Algılama Dosya Yönetim Sunucu Adresi	:		Port : 0				

Genel Ayarlar

Algılama Ayarları

CPU Kullanım Limiti : 10

Aracı CPU kullanımını aşılırsa uyarı ver 50 %

Sistem CPU Kullanımı 0 %

Duraklama Döngüsü : Yok

Güncelleme Ayarları

Java güncellemesi : Etkin

Log Ayarları

Log Yedekleme Döngüsü : Yok

Log Temizleme Döngüsü : Her gün geçmiş 1 Saat de 0 dakika

Log Temizleme Ayarları : Zamana Dayalı Log Otomatik Temizleme 0 Gün

Kapasiteye Dayalı Log Otomatik Temizleme 100 Mbyte(s)

Yönetim Görünümü

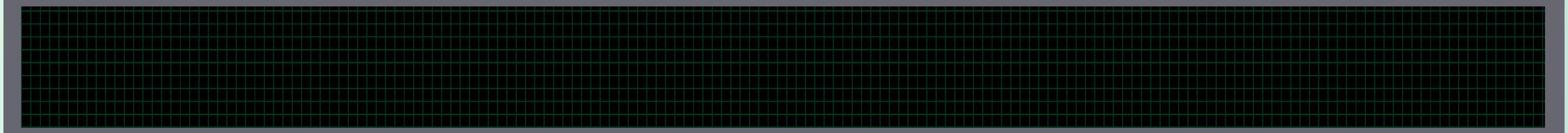
Kaynak Durumu İzleme

Bilgi

WARSS >IIS >(6)WIN-1GC3MUENMTA

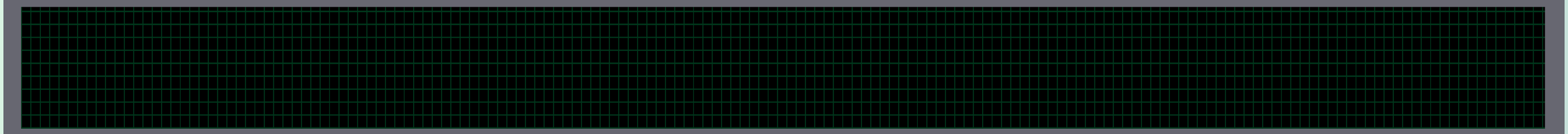
Aracı Bilgileri | Sistem Bilgisi | Kaynak Durumu

Aracı CPU Kullanımı



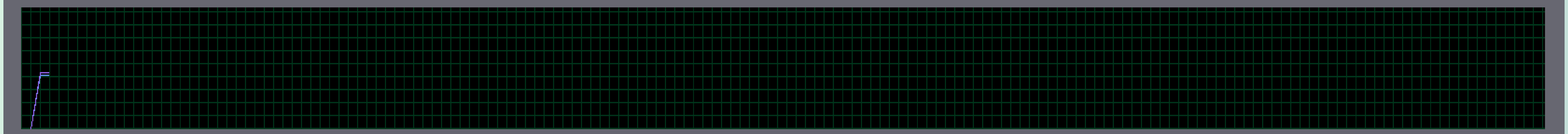
Aracı CPU Kullanımı : **0.0%**

Sistem CPU Kullanımı



Sistem CPU Kullanımı : **0.0%**

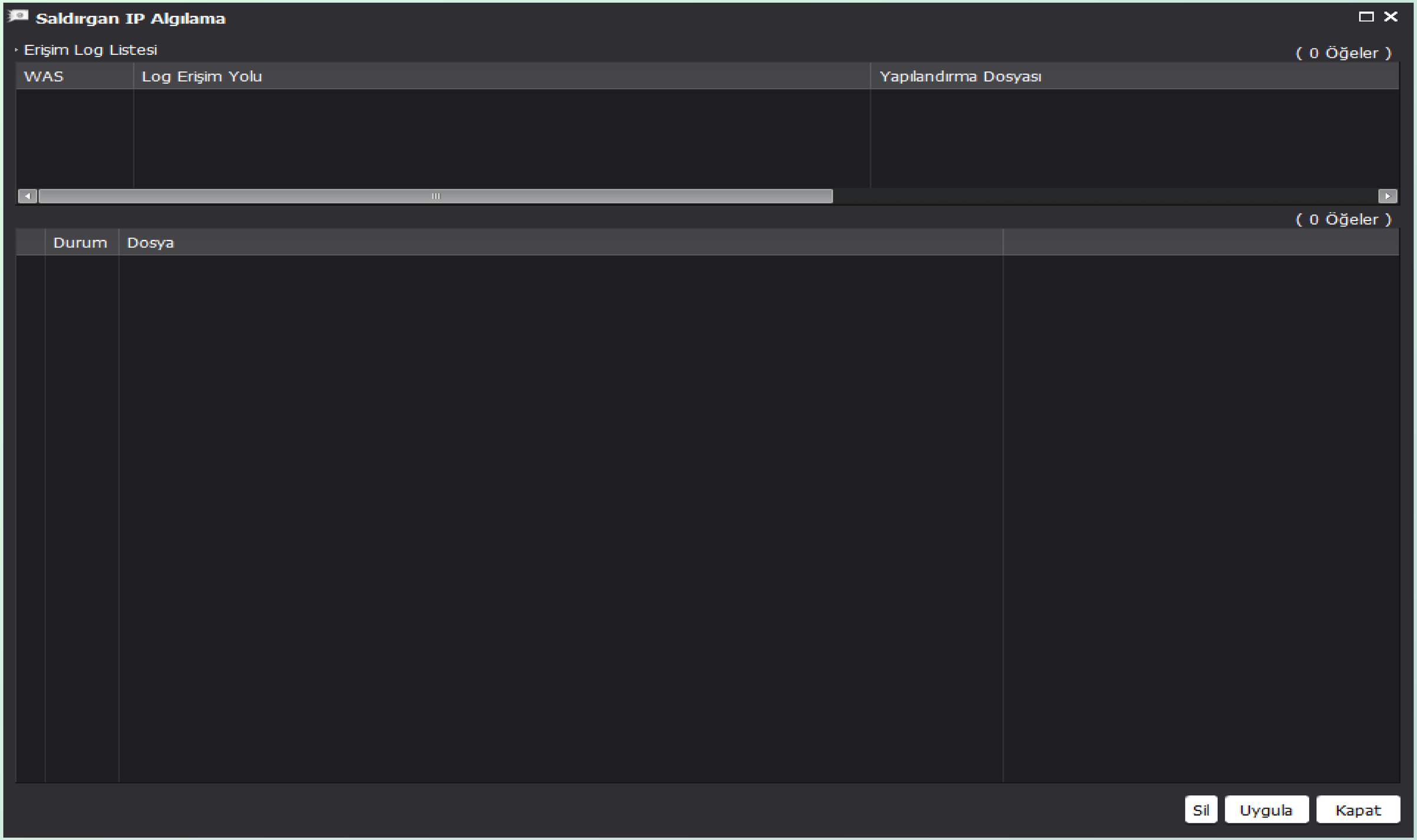
Hafıza



Fiziksel Bellek		Sanal Bellek		Hard Disk	
Kullanım Oranı	: 44.9%	Kullanım Oranı	: 47.3%	Kullanım Oranı	: 54.0%
Toplam	: 2047.4MB	Toplam	: 41.4MB	Toplam	: 19.6GB
Kullanılmış	: 919.3MB	Kullanılmış	: 19.6MB	Kullanılmış	: 10.6GB
Mevcut	: 1128.1MB	Mevcut	: 21.8MB	Mevcut	: 9.0GB

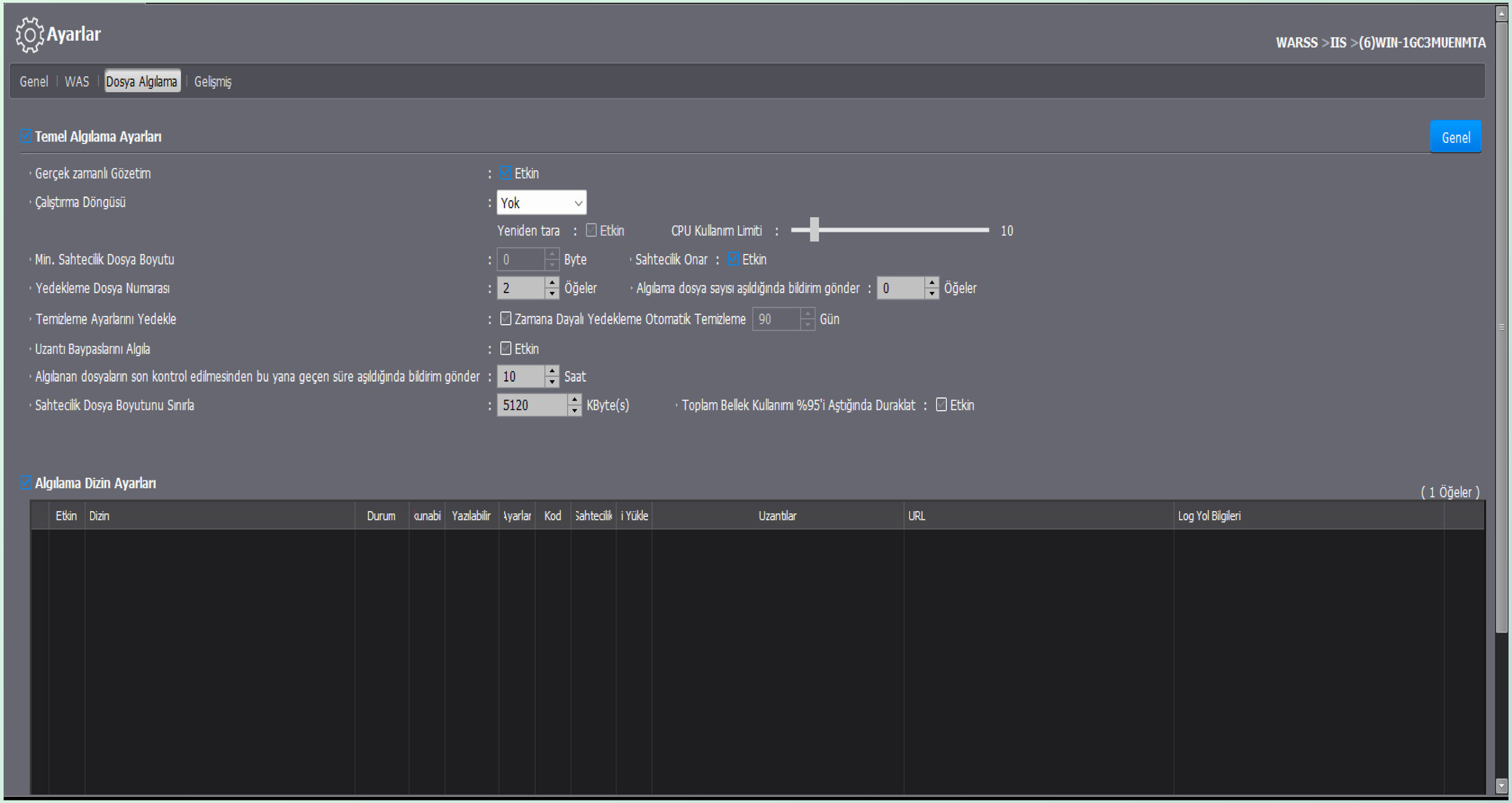
Yönetim Görünümü

Saldırgan IP Tespiti



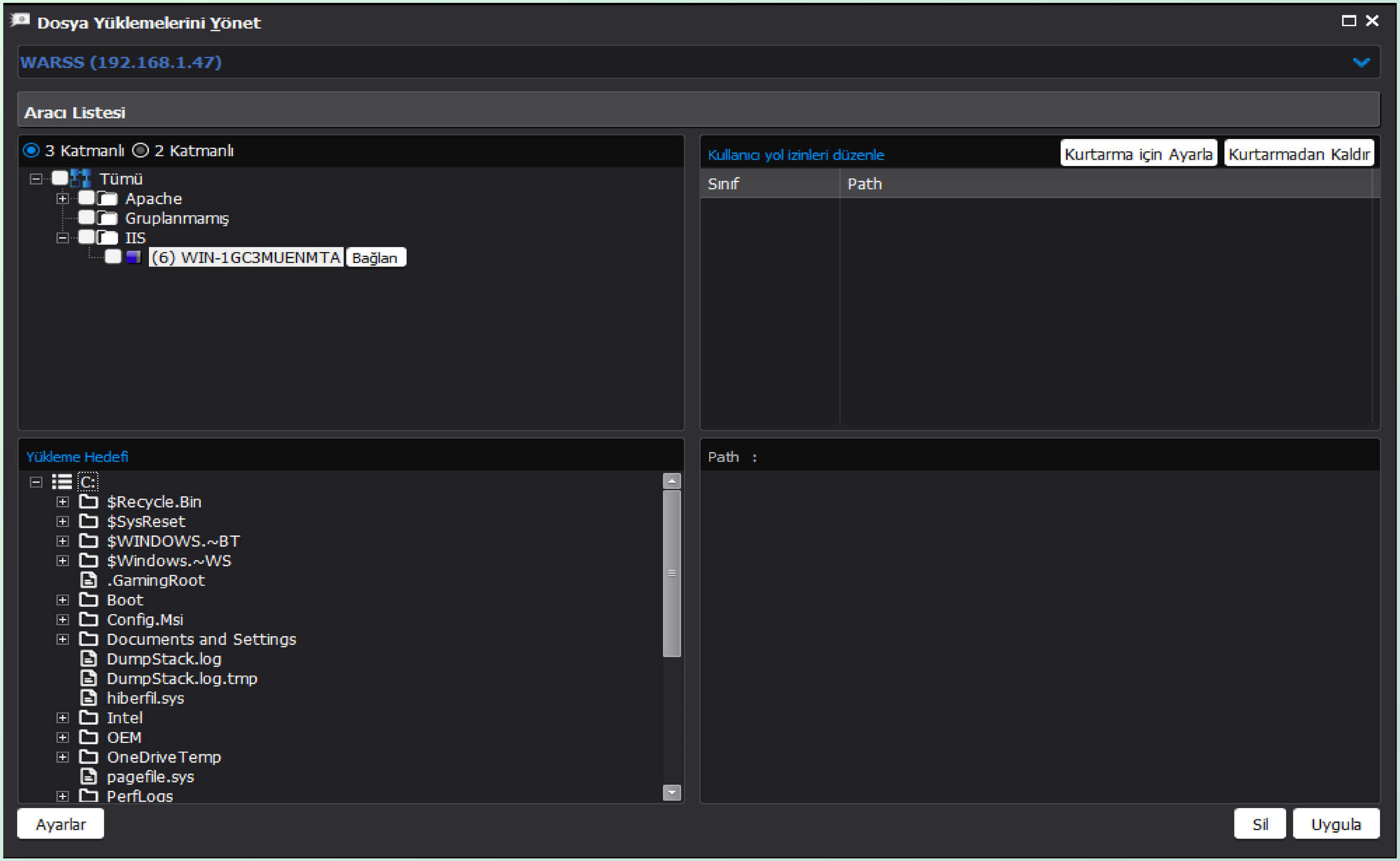
Yönetim Görünümü

Tercih Yönetimi



Yönetim Görünümü

Özel Güvenli Yükleyici



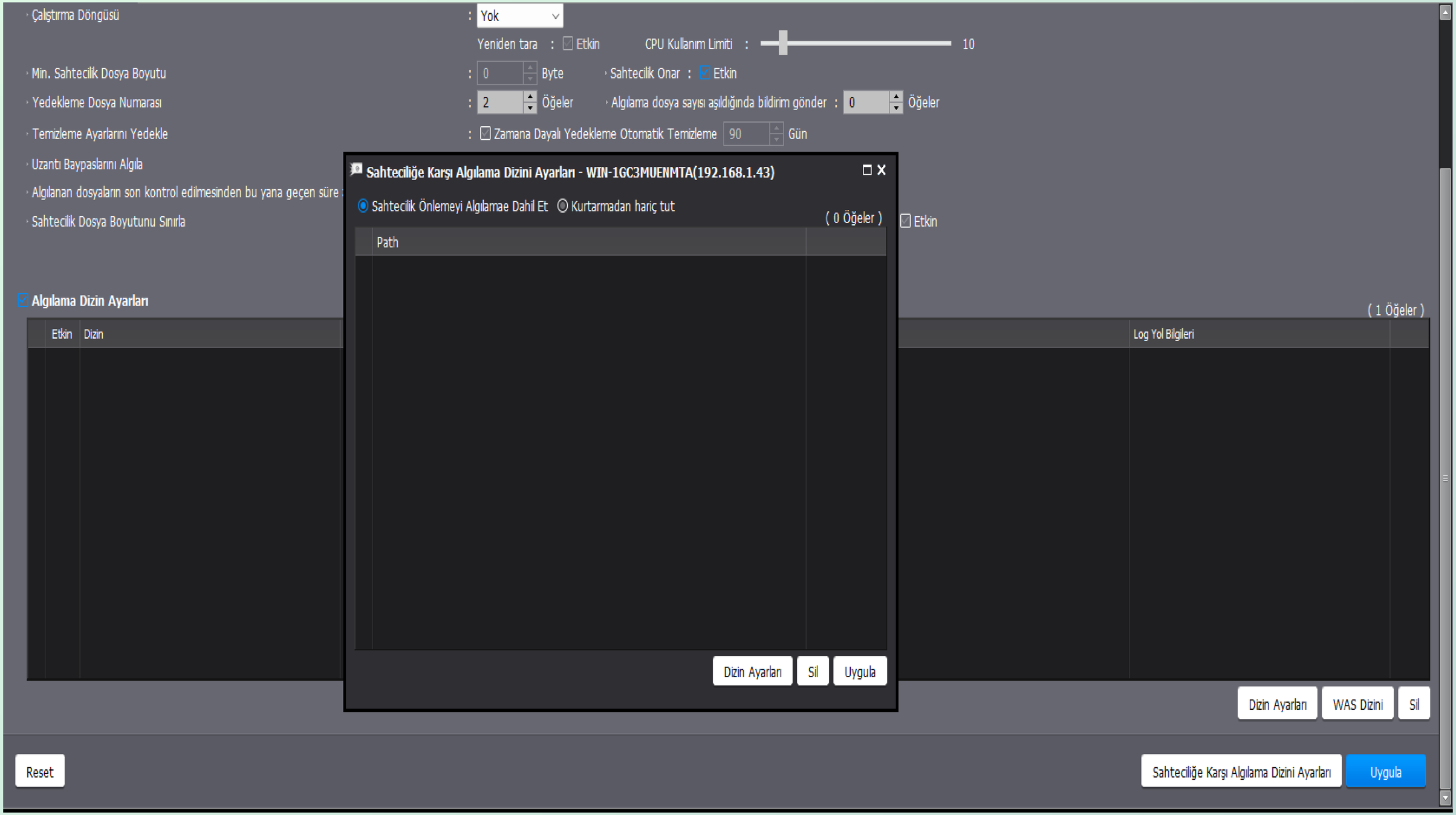
WARSS İşlevleri

Bulut Bilişim Desteği

İşlev Adı	Açıklama
Ölçek Giriş/Çıkış	• Ölçek büyütme sırasında yeni tespit hedeflerinin otomatik kaydı; tespit otomatik olarak başlar • Ölçekli olarak silinen Ajanlar için algılama/değiştirme/silme günlüklerinin yönetim sunucusuna otomatik yedeklenmesi
Ev Rehberi Arama	• Web/WAS ana dizinindeki değişiklikleri/eklemeleri bulmak için tespitleri zamanlama • Giriş dizininin ekleme/değiştirme geçmişini görüntüleme
Tarih Yönetimi	Temsilci işlem durumu ve geçmiş yönetimi (yükleme, silme, başlatma/durdurma, vb.)
Olay Çoğaltma Önleme	Ana dizin NAS alanına dahil edildiğinde yedekli sistemlerde yinelenen algılama olaylarının meydana gelmesini önleyin

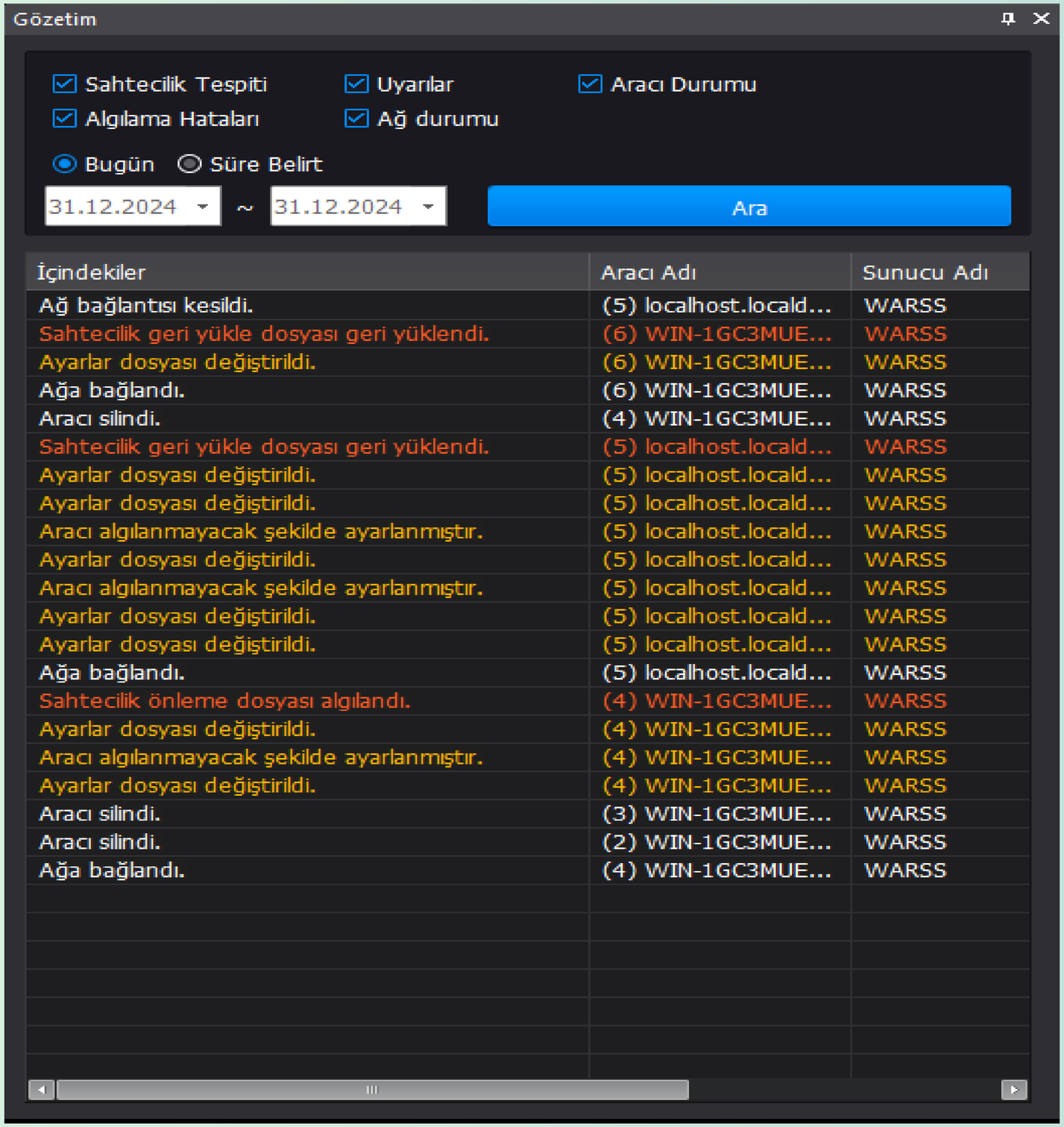
Bulut Ayarları Görünümü

Ev Rehberi Arama



Bulut Ayarları Görünümü

Kayıt/Tarih Yönetimi



WARSS Şirket İçi Yapılandırma Şeması