

umv

WARSS

**Website Attack Restoration
Security Solution**

Gerçek zamanlı web sitesi güvenliği



içindekiler

01

Hakkımızda

02

Web Hacking
Trendleri

03

Problemler

04

WARSS

05

Kullanım
Durumları

06

Soru & Cevap

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>

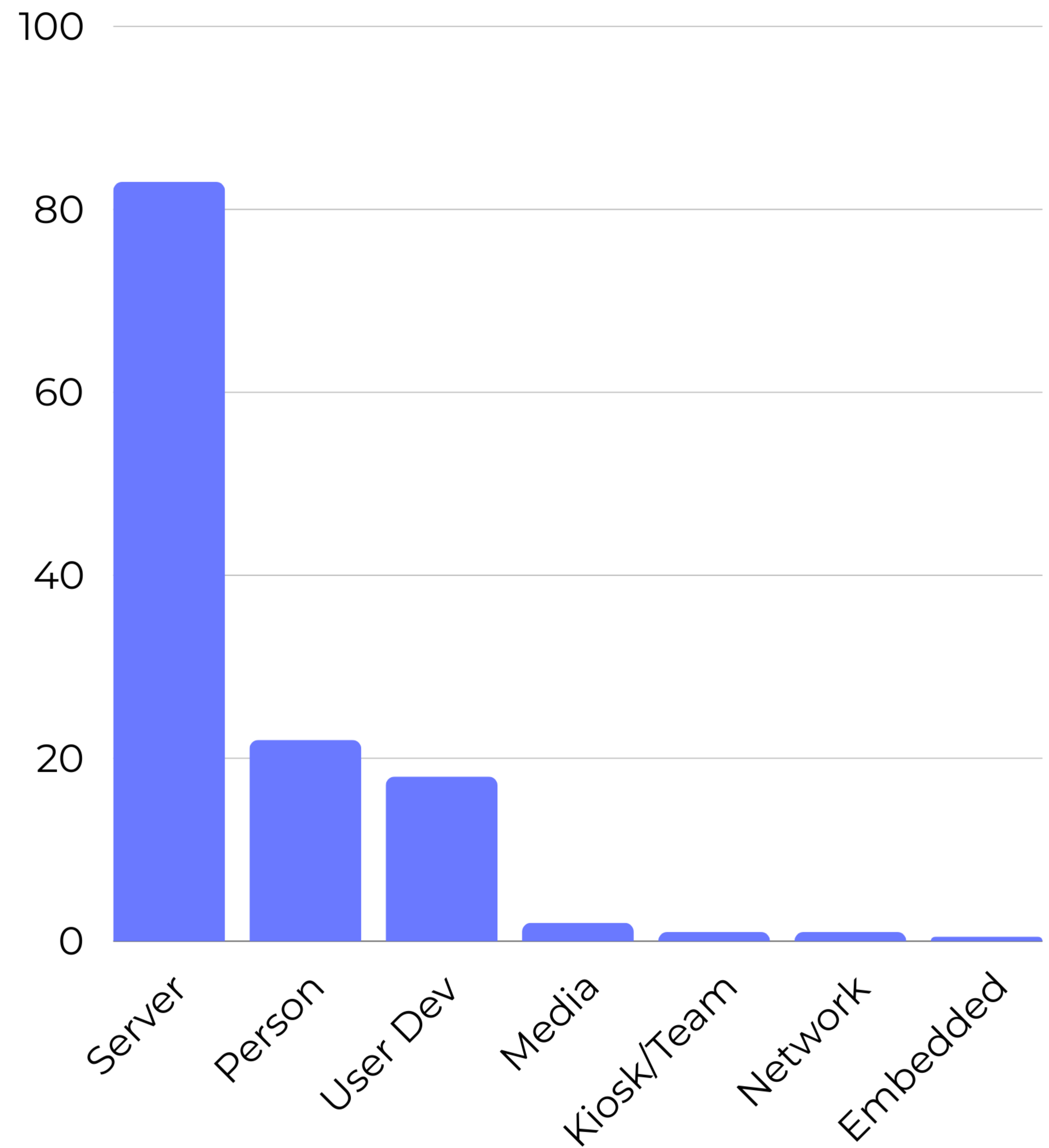
Web Korsanlığı Artışta

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

BREAKING

[Image Source: The Record](#)

PERVOKLASSNIY RUSSIAN HACKERS ATTACK

11 mins ago

CHARITY

COURT

CRIME

ECONOMY

EDUCATION

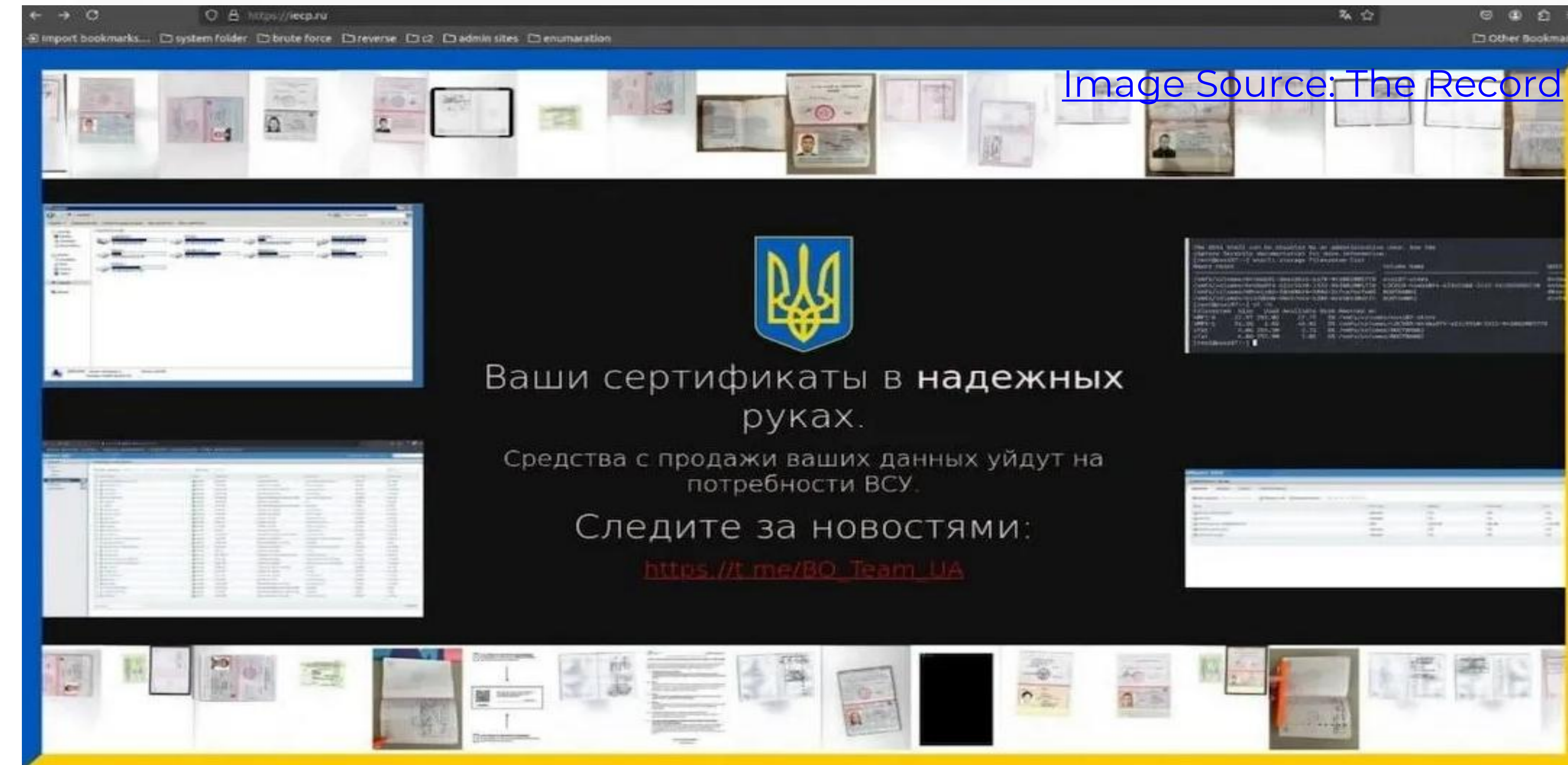


By Даниел Хопкинс

Share



No Comments



[Image Source: The Record](#)

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

[Image Source: Hack Read](#)



Internet Archive is a non-profit library of millions of free texts, movies, software, music, websites, and more.



Search

Advanced Se

New to the Archive?

How to search the



How to download files



Listening to music on the

Terms of Service (last updated 12/31/2014)

Trend: Hacktivizm ve Siber Terörizm

- **Siyasi** 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 finansmanı**yla 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](#)

Problemler

Tahrip Etme Yöntemleri

1. Kaynak Kodunda Değişiklik

Bitcoin, eh? Never heard of it. But perchance you would like to try something better. Something with more "zing". Something named CosbyCoin!

Continue =>

crash.. Holding my Cosbycoin.	bitjet	2	333	Today at 07:33:43 pm by kjj
	WiseOldOwl	9	402	Today at 07:32:21 pm by ShadowOfHarbringer
tfom to Mt Gox. Anybody interested? = 1	4xCoder	24	1564	Today at 07:32:20 pm by AlexZ
	mizerydiana	17	562	Today at 07:19:34 pm by ssaCEO
Image Source: alphavilleherald.com		17	1501	Today at 06:58:32 pm by enmaku

buttcoins.org




FUCK! KOREA

Deploy the Sade missile system is ignorant
Lotte group is too naive!
Cherish peace, stay away from war!
Boycott lotte, resisit Sade!
lotte,get out of China! Korea sticks fuckyou!

犯我中华者虽远必诛!

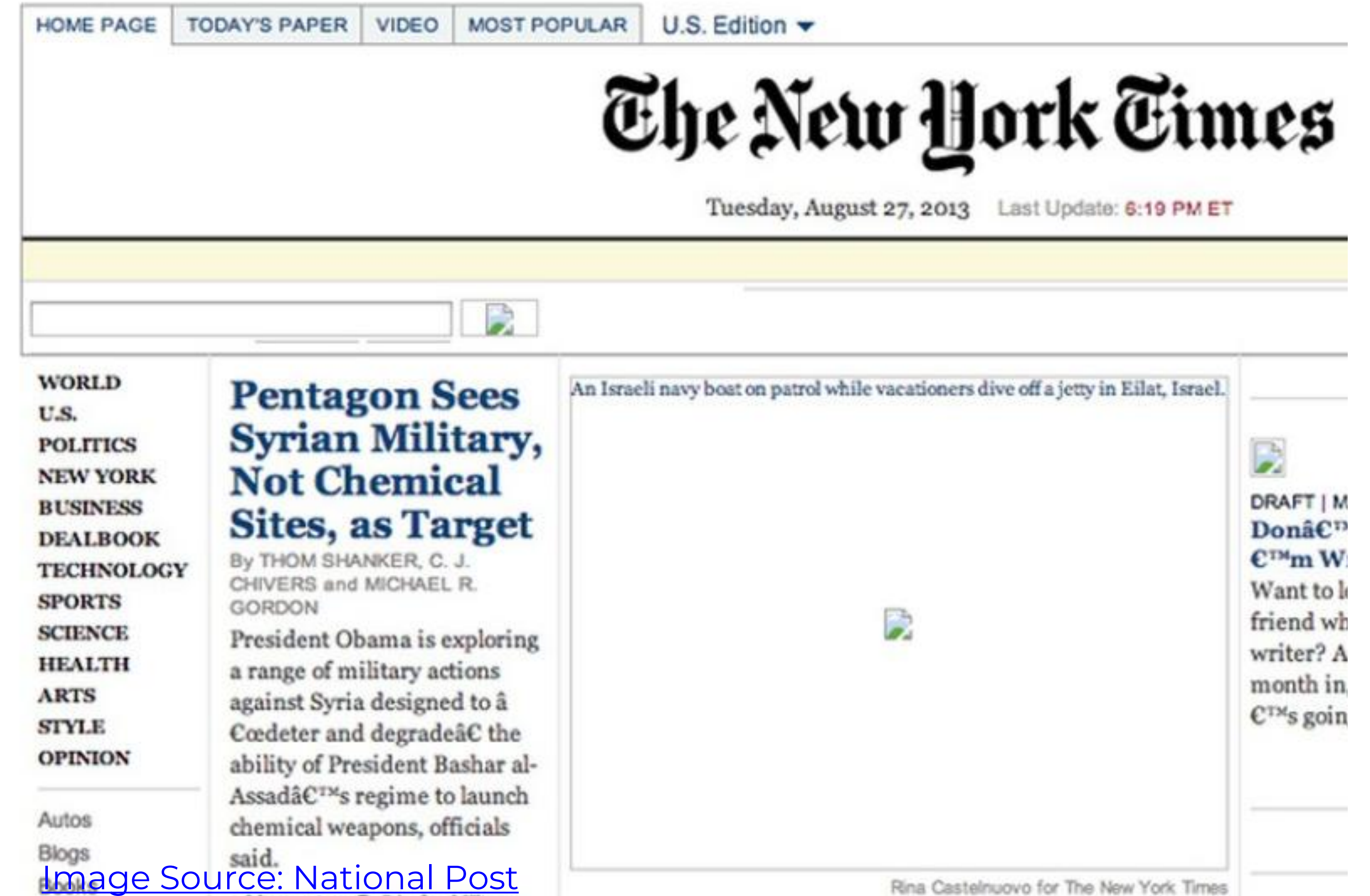
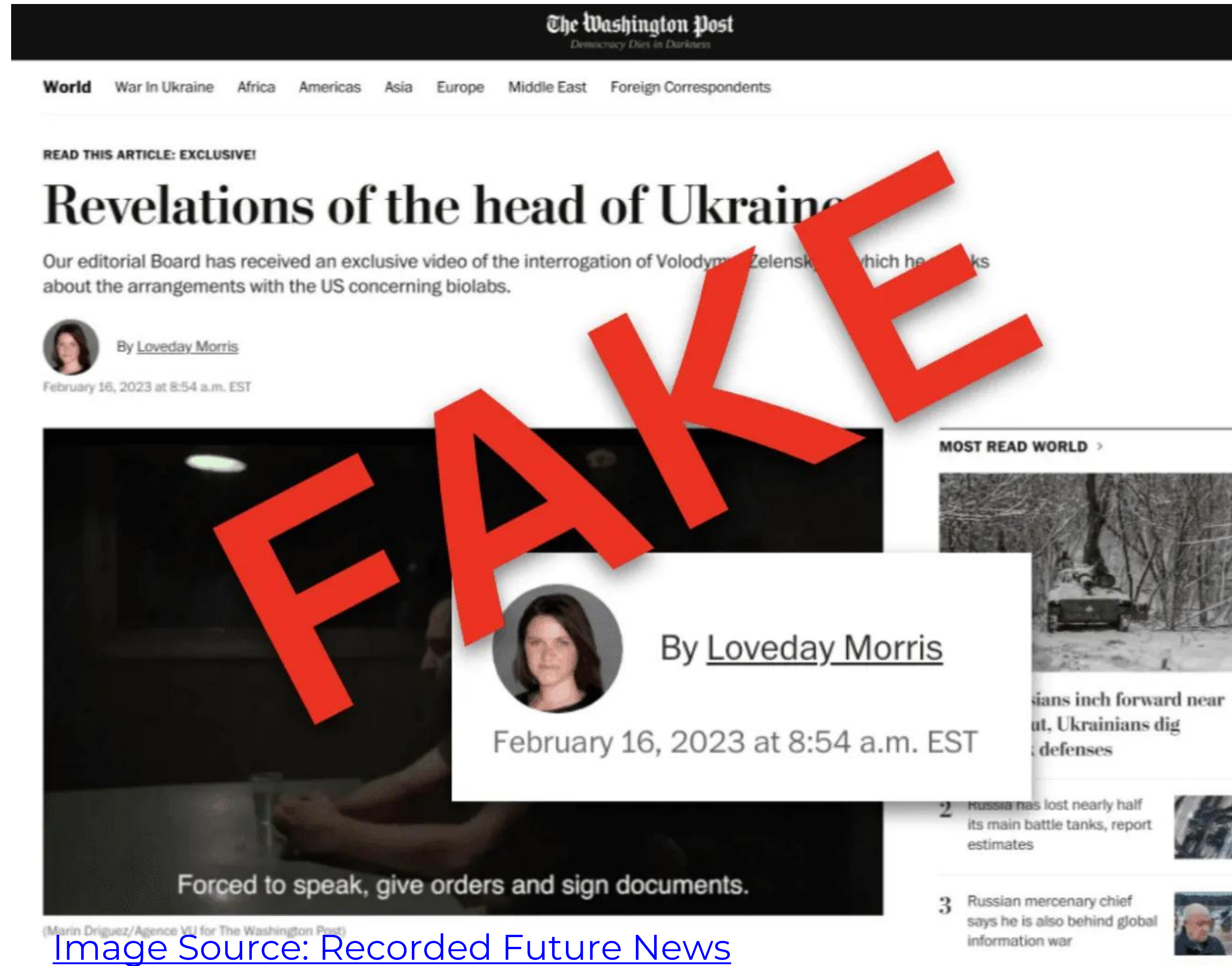


보안뉴스 Intelligence Bureau

Image Source: boannews.com

Tahrip Etme Yöntemleri

2. İçerik Sahtekarlığı/Enjeksiyonu

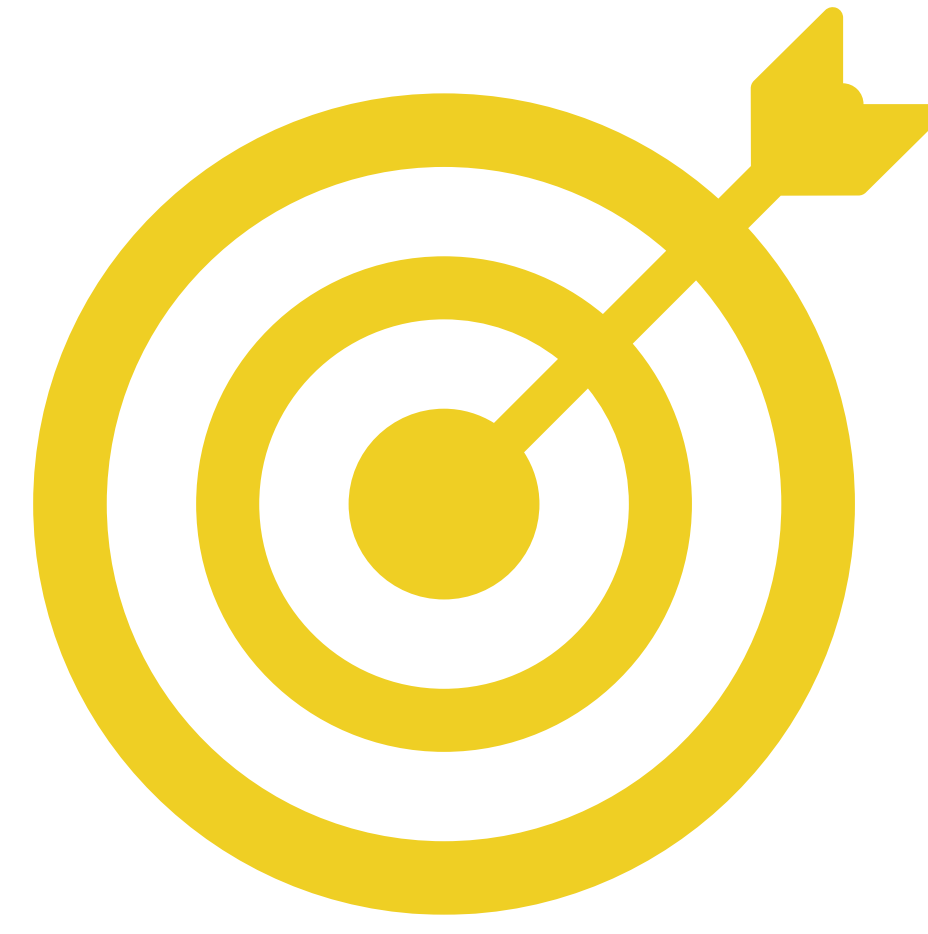


Neden Tahrif Ediliyor?



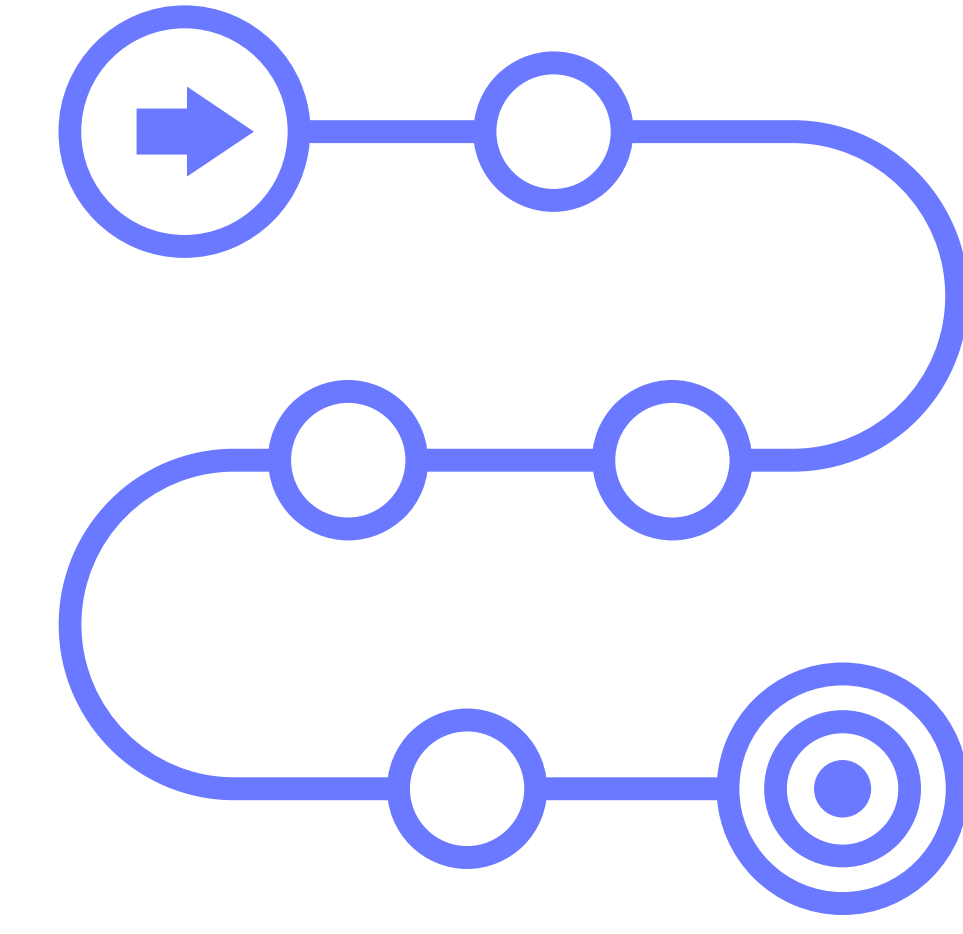
Motivasyon

- hacktivism
- utanç
- şöhret/tanınma
- siber terörizm



Hedef

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

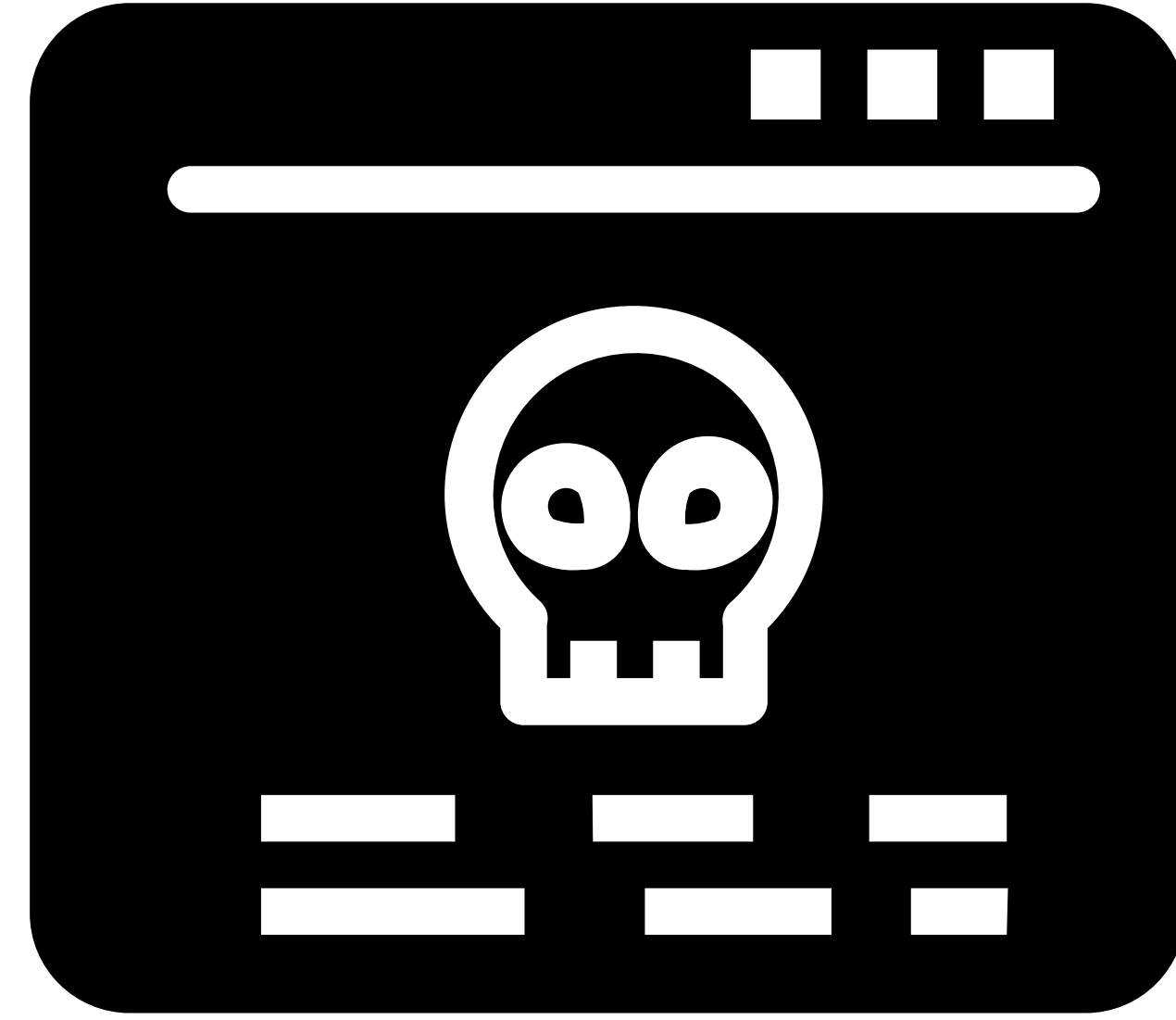
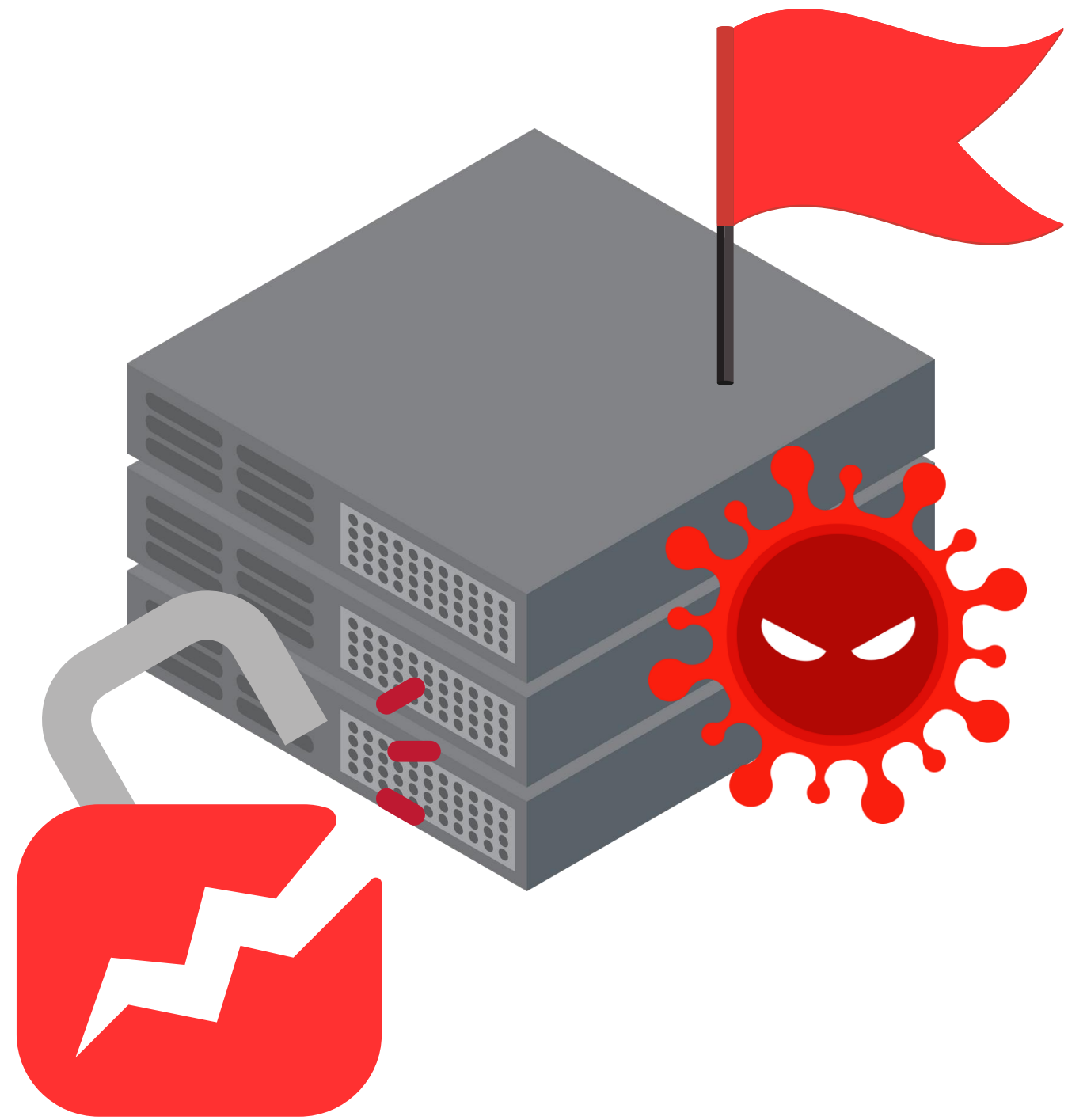


Yöntem

Web tabanlı bileşenlerdeki zayıflıklardan yararlanır:

- web sunucusu
- web uygulamaları
- web siteleri

Bir Web Saldırısının Anatomisi



Etki

3

- Tahrifat
- Kaynak kodu ve içerik sahteciliği

Yükselme

2

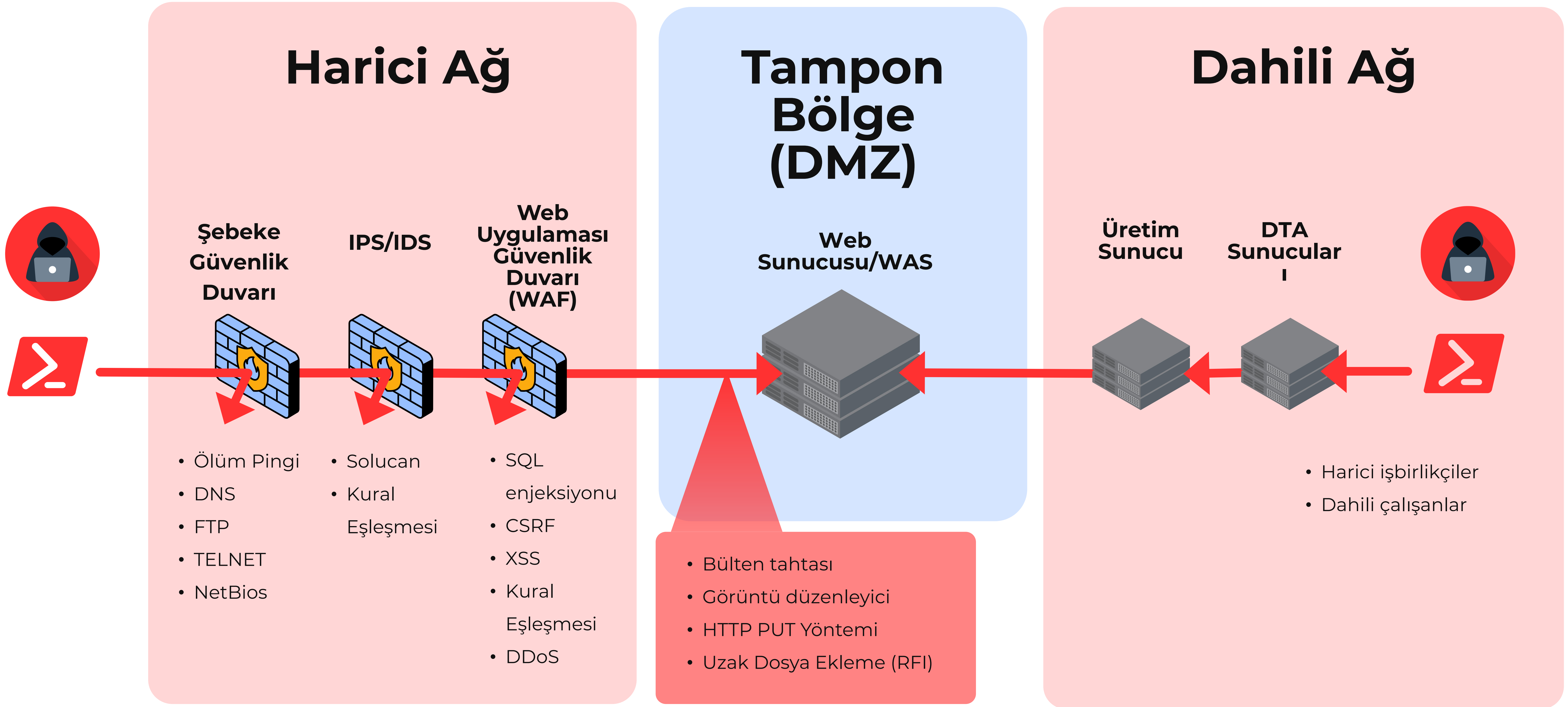
- Varlık oluşturmak için web sunucusuna yüklenen kötü amaçlı yazılım
- Web sunucusu dosyalarını değiştirmek için çalıştırılan ek kötü amaçlı yazılım (yük)

Sızma

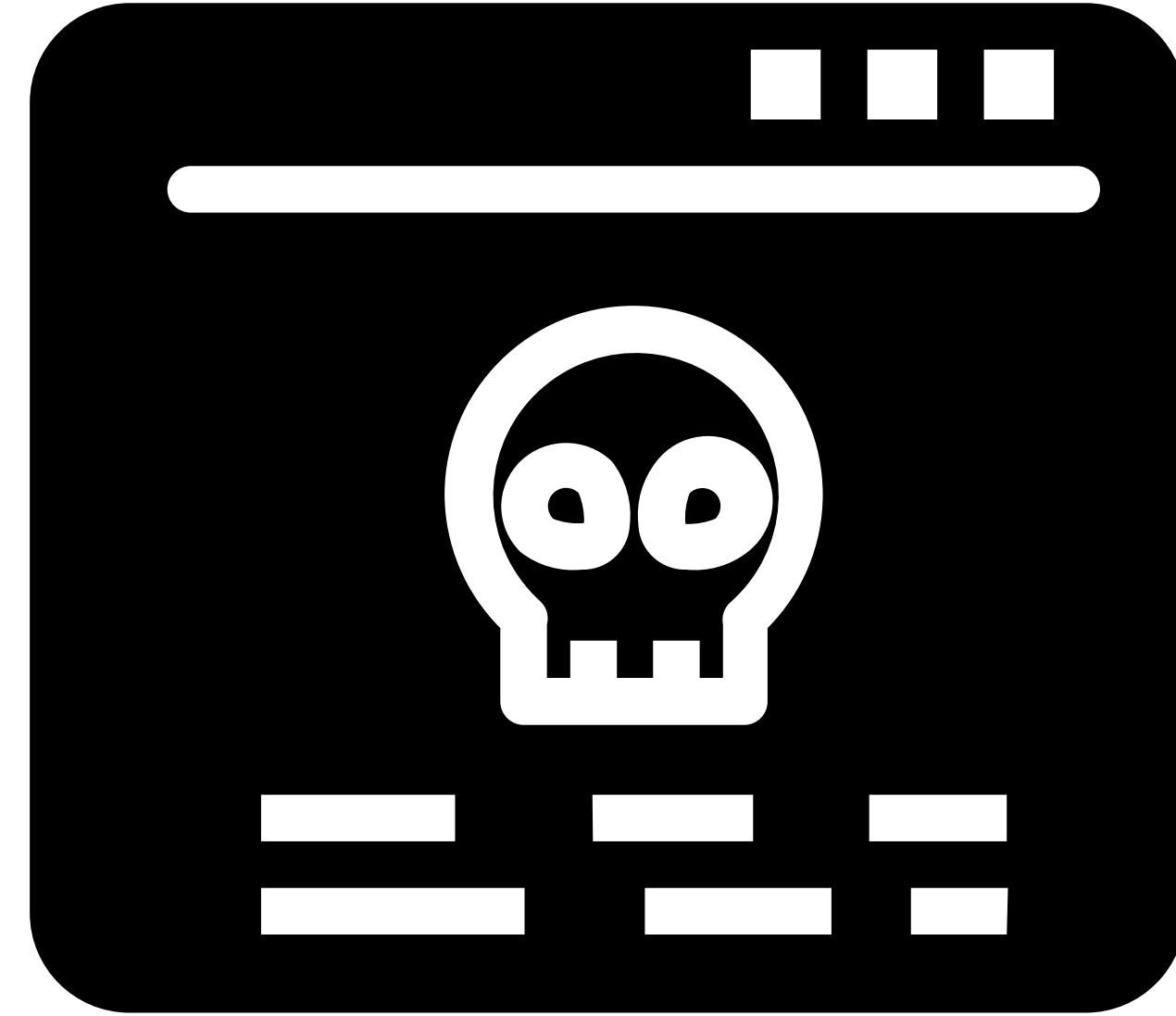
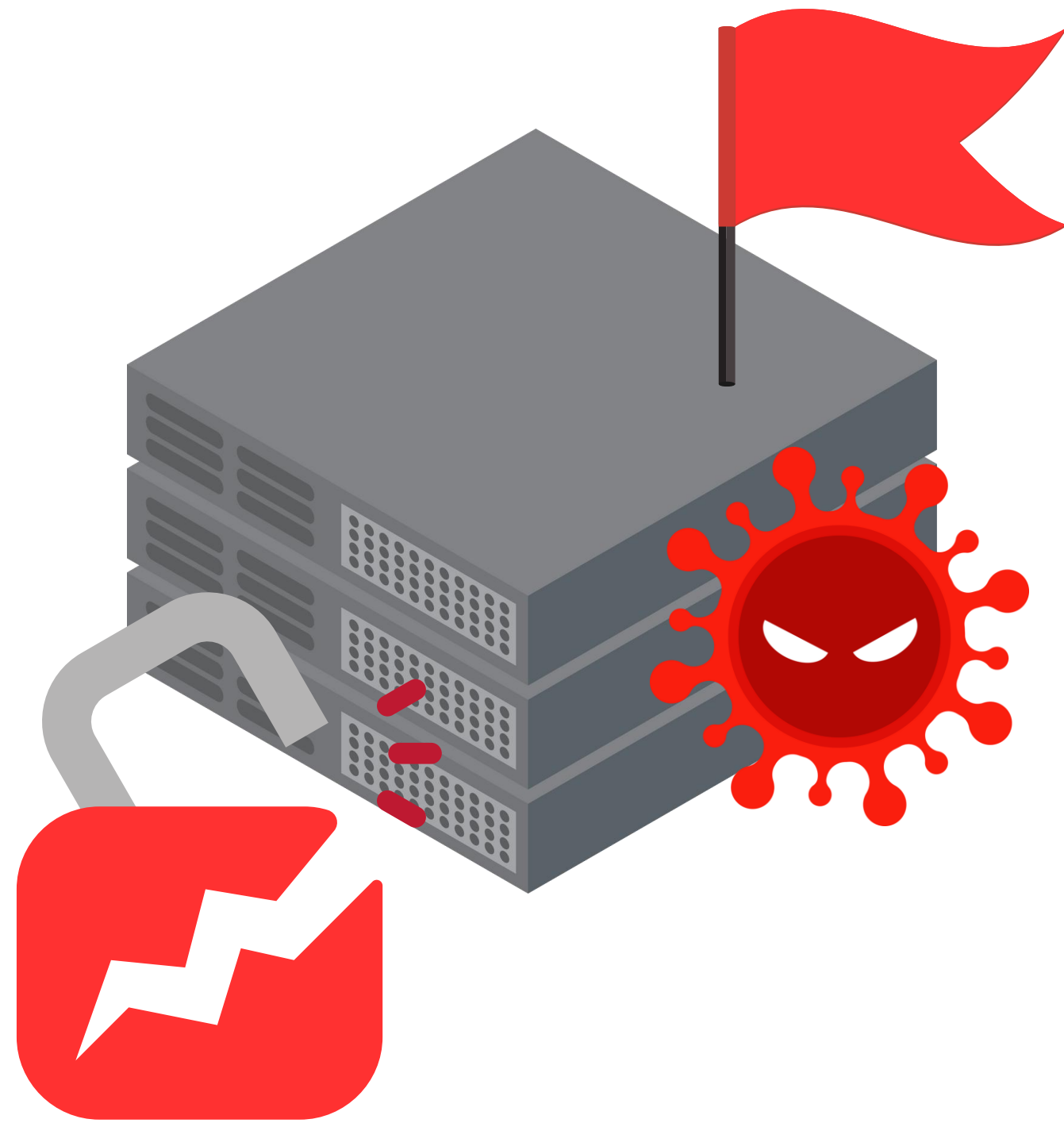
1

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

Mevcut Durum



Bir Web Saldırısının Anatomisi



Etki

3

- Tahrifat
- Kaynak kodu ve içerik sahteciliği

Yükselme

2

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

Sızma

1

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

- («Web siteniz 'saldırgan' tarafından hacklendi. Panik yapmayın, e-postamla iletişime geçin ve bunu çözelim. Siteyi tekrar düzeltseniz, web sitenizi silmiş olsanız bile Shell arka kapıma hala erişebileceğimi unutmayın»

your website has been hacked by [REDACTED], don't panic
contact my email and we will solve it well remember
even if you fix it again I can still access my
shell backdor even though you have deleted your website, it is not sturdy

Contact Me [REDACTED] : [REDACTED]@gmail.com

<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 Attack Restoration & Security Solution (WARSS)

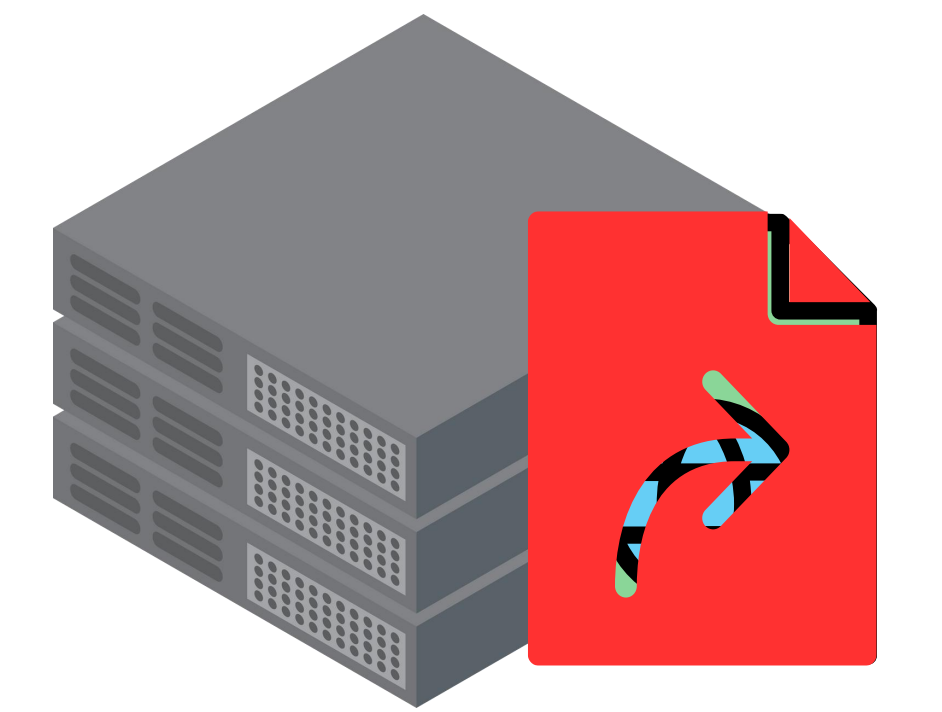
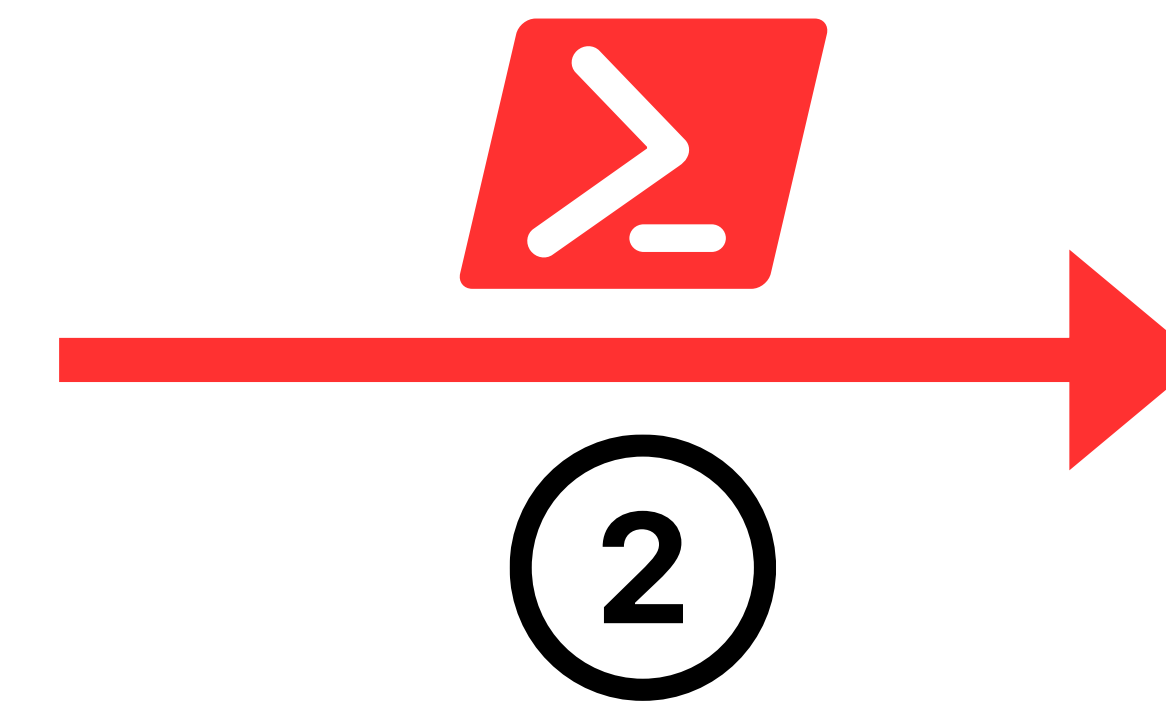
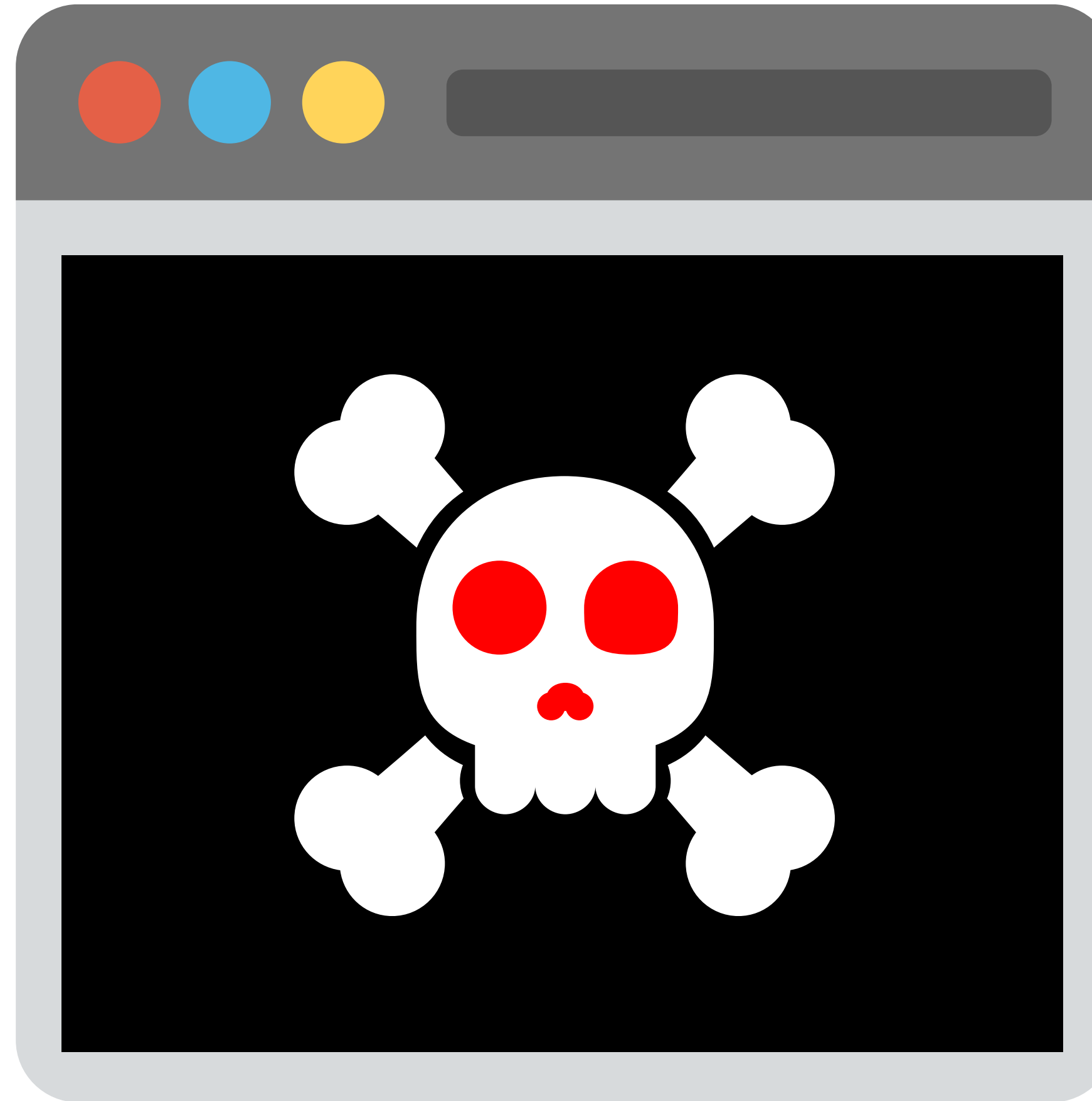
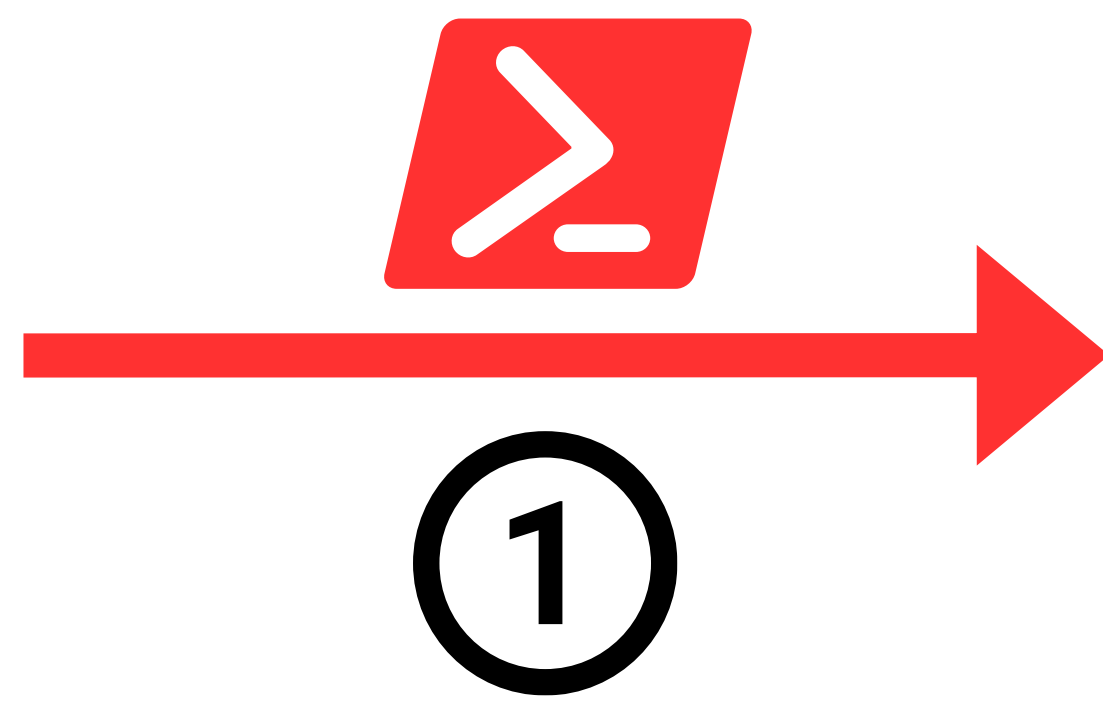
Bir web sitesindeki yetkisiz deęişiklikleri **tespit** eden ve orijinal dosyaları **gerçek zamanlı** olarak **geri yükleyen** web sunucusu güvenlik güçlendirici çözümü



Web Sitesi Tahrifatı Nasıl Gerçekleşir?

savunmasız web sitesi

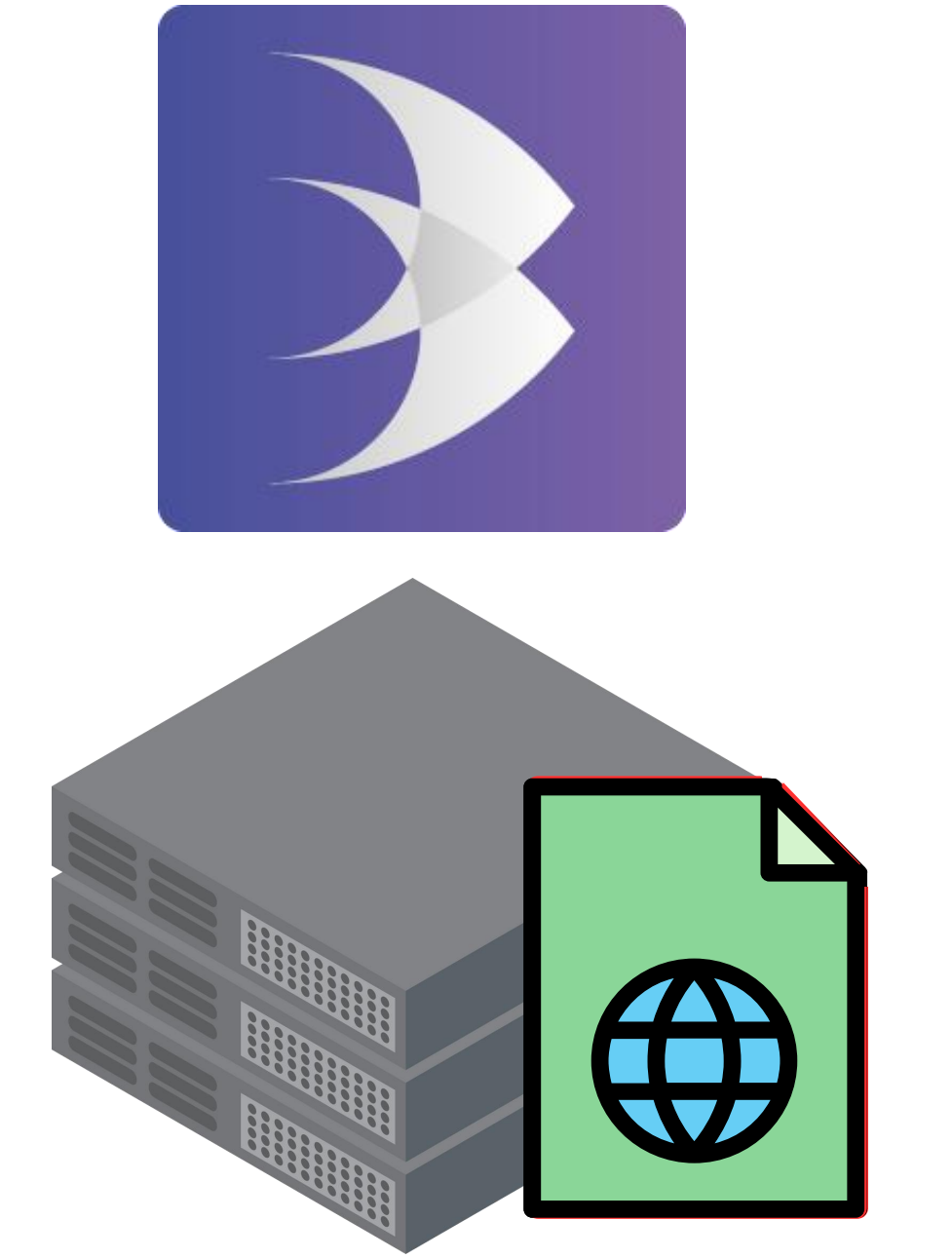
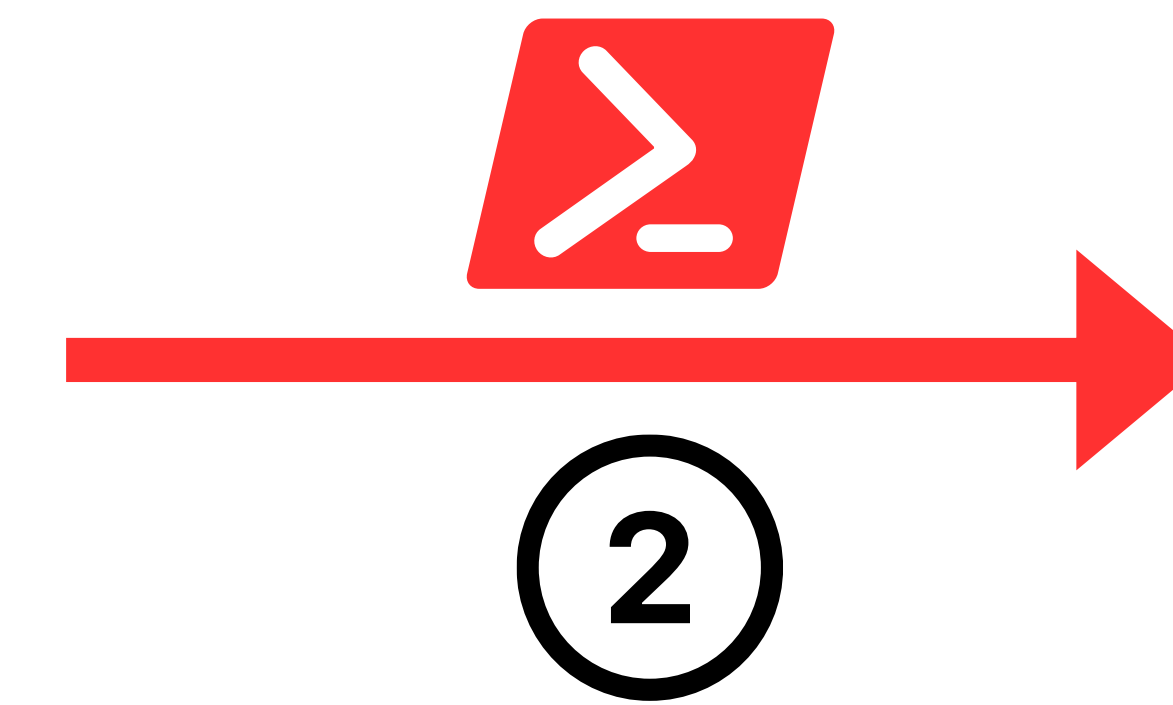
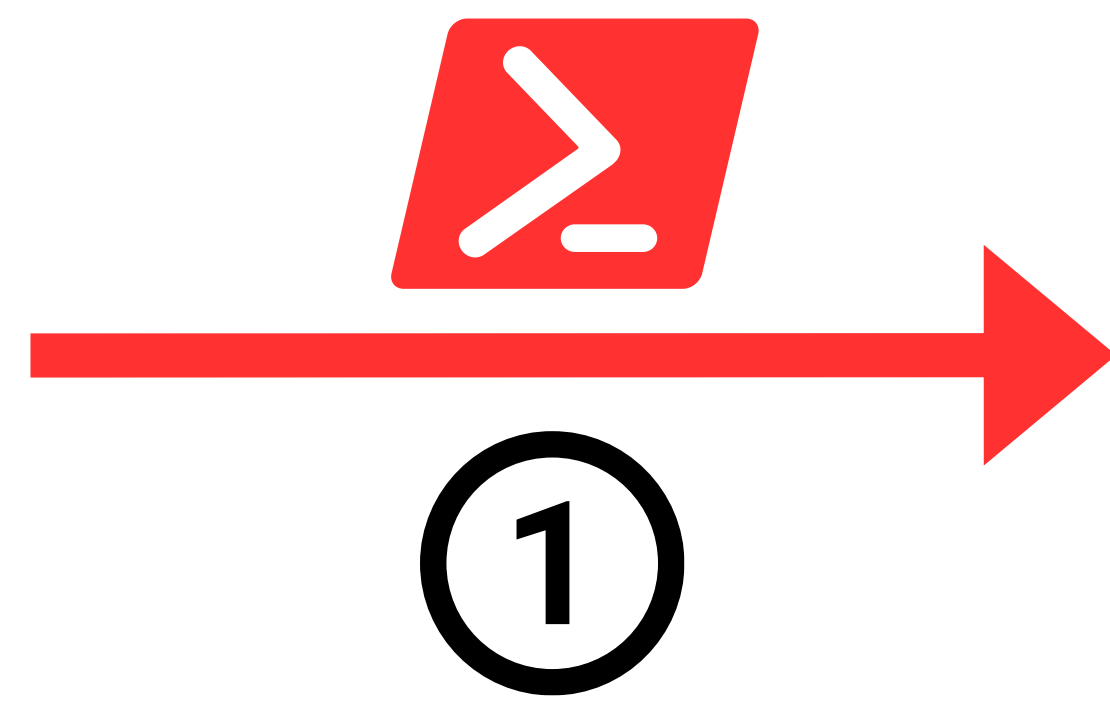
web sunucusu



WARSS Nasıl Çalışır?

savunmasız web sitesi

web sunucusu



Demo

The screenshot displays the WARSS 2.7.0.4 interface. The main window is a terminal window connected to 192.168.1.40. The terminal shows the following commands and output:

```
[root@localhost html]# ll
total 4432
-rw-r--r--. 1 root root 279 Jun 11 05:58 index_2.html
-rw-r--r--. 1 root root 281 May 31 04:14 index.html
-rw-r--r--. 1 root root 1682529 Jun 11 05:24 resim1.png
-rw-r--r--. 1 root root 2844197 Jun 11 05:24 resim2.png
drwxr-xr-x. 2 root root 42 Jun 11 07:51 warss1
drwxr-xr-x. 2 root root 42 Jun 25 08:14 warss2
[root@localhost html]# cp -R index_2.html warss1/index.html
cp: overwrite 'warss1/index.html'? y
[root@localhost html]# cp resim2.png warss1/
[root@localhost html]# cp -R index_2.html warss2/index.html
cp: overwrite 'warss2/index.html'? y
[root@localhost html]# cp resim2
```

The interface also includes a file explorer on the left showing the directory structure of the terminal session, and a 'Monitor' window on the right displaying a list of events:

Contents	Agent Name	Server Name
The Restore Anti-Falsification file has been rest...	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Network connected.	(1) localhost.locald...	WARSS

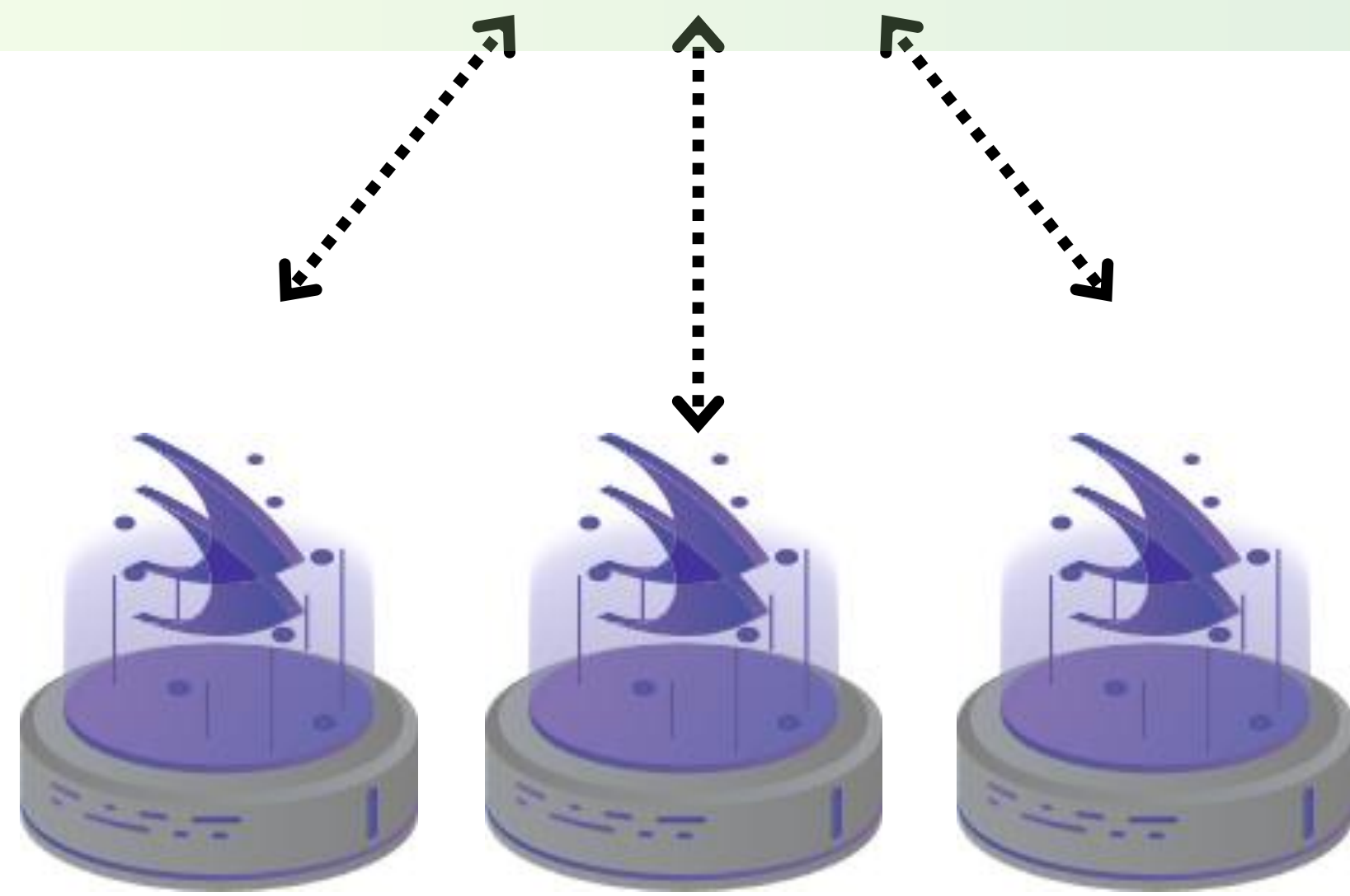
<https://www.youtube.com/watch?v=B20LDk0iAJQ>

WARSS Yapılandırması



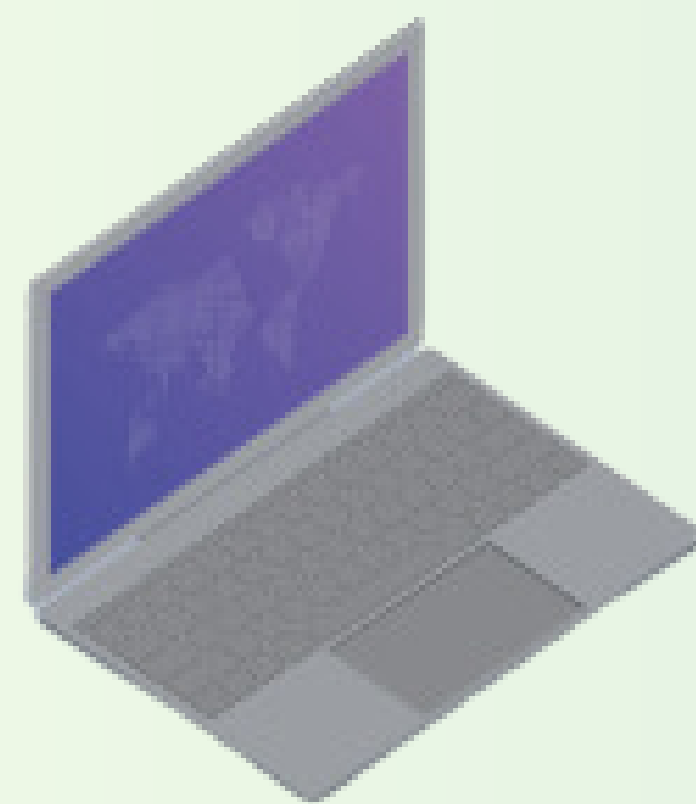
WARSS Yönetim Sunucu(ları)

- 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

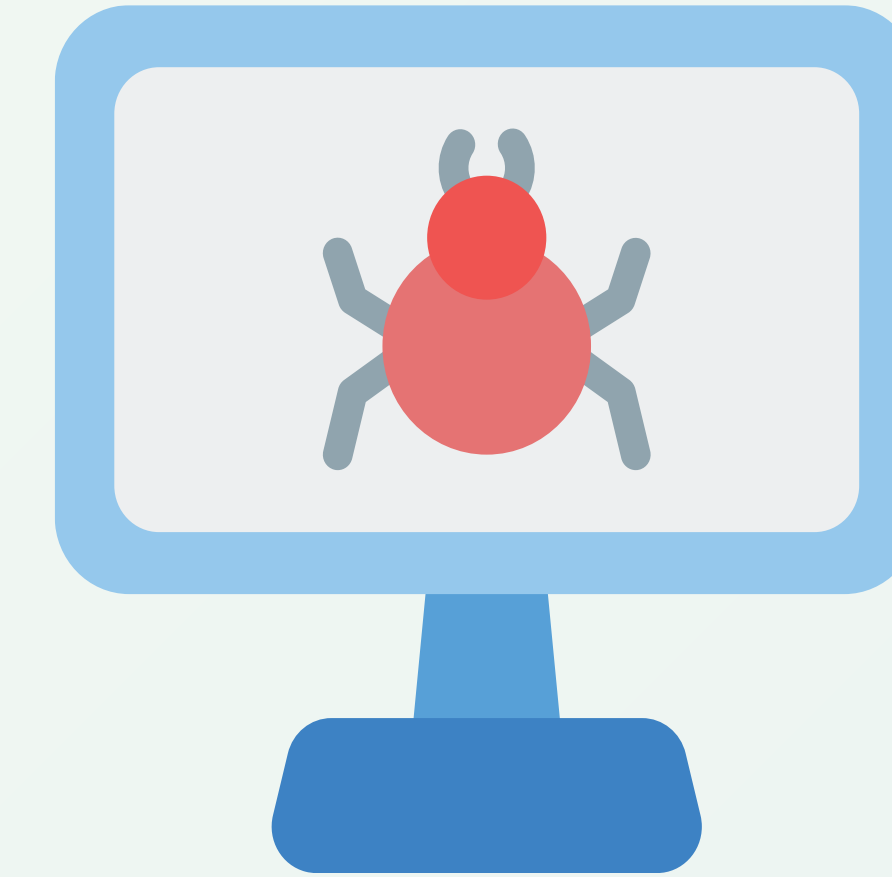
- Yönetici bilgisayarında yüklü program
- Şunlar için ayarları kontrol eder: algılama, uzaktan eylem, ortam ve raporlama
- Yönetim, istatistik ve raporlama ayarlarına erişim

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. ihlal olduğunu varsayalım

SIFIR GÜVEN

3. ihlal olduğunu varsayalım



Gerçek zamanlı
algılama

Kolaylaştırılmış
yönetim

Hızlı hafifletme

Gerçek zamanlı dosya
değişikliği izleme

Gerçek zamanlı
uyarılar ve raporlar

Otomatik restorasyon
ve kurtarma



Uygunluk
bilgiye ihtiyaç
duyulduğunda erişilebilir

ISO/IEC 27001
Prensipileri

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 güvenliđi 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) (iyi 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

The screenshot displays the WARSS interface with a 'Change Prevention History' window for a Windows system (192.168.0.123). The interface shows a table of detected files and their details, including file paths, dates, and file information before and after modification. A 'Details' section provides a side-by-side comparison of the file's content, highlighting changes in the code.

Row	Column	Status
1	1	Dele...

Change Prevention Information

2022-07-13 09:54:26

- Detected File : C:\Users\Wlc\Desktop\www\main.php
- Date : 2022-07-13 09:54:26

File Information Before Modification	File Information After Modification
File Time : 2014-04-01 09:53:42	File Time : 2022-07-13 09:54:23
File Size : 5,182 Bytes	File Size : 4,192 Bytes

Details

Modified File : 2022-07-13 09:54:26

```

1
2 {
3 ?>
4
5 <script language="javascript">
6 //document.location.href = 'main.php';
7 document.location.href = 'http://www.10asia.co.kr/main.php';
8 </script>
9
10 <?
11     exit
12 }
13

```

Original File

```

13 if( !$g_strLibDir ) $g_strLibDir
14 if( !$g_strLibDir ) { echo 'Ser
15 include ($g_strLibDir . '/glob
16 include ($g_strLibDir . '/glob
17
18 require_once $g_strIncDir . '
19
20 $strCssDate = '';
21 $strCssDate = '20091111';
22
23 if($_SERVER['HTTP_HOST'] =
24 {
25 ?>
26
27 <script language="javascript">
28 //document.location.href = 'main.
29 document.location.href = 'http://w
30 </script>
31
32 <?
33     exit
34 }
35

```

<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 Ajansı yüklendi

Sürekli Koruma

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

The screenshot displays the WARSS interface with the following details:

- Change Prevention History - WINDOWS(192.168.0.123)**
- Change Prevention Information**

Time	Detected File	Date
2022-07-13 09:54:26	C:\Users\Wlc\Desktop\www\main.php	2022-07-13 09:54:26
- File Information Before Modification**
 - File Time : 2014-04-01 09:53:42
 - File Size : 5,182 Bytes
- File Information After Modification**
 - File Time : 2022-07-13 09:54:23
 - File Size : 4,192 Bytes
- Details**

Row	Column	Status	Modified File : 2022-07-13 09:54:26	Original File
1	1	Dele...	<pre>1 { 2 { 3 ?> 4 5 <script language="javascript"> 6 //document.location.href = 'main.php'; 7 document.location.href = 'http://www.10asia.co.kr/main.php'; 8 </script> 9 10 <? 11 exit 12 } 13 }</pre>	<pre>13 if(!\$g_strLibDir) \$g_strLibDir 14 if(!\$g_strLibDir) { echo 'Ser 15 include (\$g_strLibDir . '/glob 16 include (\$g_strLibDir . '/glob 17 18 require_once \$g_strIncDir . ' 19 20 \$strCssDate = ''; 21 \$strCssDate = '20091111'; 22 23 if(\$_SERVER['HTTP_HOST'] = 24 { 25 ?> 26 27 <script language="javascript"> 28 //document.location.href = 'main. 29 document.location.href = 'http://w 30 </script> 31 32 <? 33 exit 34 } 35 }</pre>

WARSS'ı Kimler Kullanıyor?

WARSS birçok ulusal şirket ve kurumun itibarını korumaktadır.



... and more!

Yüzlerce Müşteri

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



13+ years



13+



7-8



Hanwha

13+



10+



Prudential

13+



TOYOTA



STARBUCKS

dun & bradstreet



SUPREME COURT
OF KOREA



Ministry of National Defense
Republic of Korea



HYUNDAI

Deloitte.

iMBC

... ve çok daha fazlası!

umv

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 2.7.0.4

Göster Yönet Pencere Yardım [Admin Adı : 관리자(smadmin)]

SAHTECİLİK KARANTİNA İSTİSNA RAPOR KAYITLAR AYARLAR BİLGİ GÖZLEM ARACILAR

Sorgula (5)localhost.localdomain (6)WIN-1GC3MUENMTA

Ara

WSS (192.168.1.47)

- Apache
- localhost.localdomain(5)
- IIS
- WIN-1GC3MUENMTA(6)**
- Gruplanmamış

Sahtecilik Önleme

Arama Ayarları

Fonksiyon : Tümü Algılama Geri Yükleme

Tarih : Son tarih Tümü Süre 31.12.2024 ~ 31.12.

Rapor Tarihi	Path	Dosya Adı
2024-12-31 11:24:47	C:\inetpub\wwwroot	ASPTotal.asp

Önleme Geçmişini Değiştir - WIN-1GC3MUENMTA(192.168.1.43)

Önleme Bilgilerini Değiştir

2024-12-31 11:24:46

Algılanan Dosya : C:\inetpub\wwwroot\ASPTotal.asp

Tarih : 2024-12-31 11:24:46

Değişiklik Öncesi Dosya Bilgileri	Değişiklikten Sonra Dosya Bilgileri
Dosya Zamanı : 2023-02-08 04:15:10	Dosya Zamanı : 2024-12-31 04:24:43
Dosya boyutu : 39,529 Byte	Dosya boyutu : 38,722 Byte

Ayrıntılar

Sıra	Sütun	Durum	Değiştirilmiş Dosya : 2024-12-31 11:24:46	Orijinal dosya
34	2	Silinen	<pre>24 function yesok() { 25 if (confirm("해당 조작을 실행할 것입니까")) 26 return true; 27 else 28 return false; 29 } 30 function ShowFolder(Folder) { 31 top.addrform.FolderPath.value = Folder; 32 top.addrform.submit(); 33 }</pre>	<pre>24 function yesok() { 25 if (confirm("해당 조작을 실행할 것입니까")) 26 return true; 27 else 28 return false; 29 } 30 function ShowFolder(Folder) { 31 top.addrform.FolderPath.value = Folder; 32 top.addrform.submit(); 33 } 34 function FullForm(FName, FAction) { 35 top.hideform.FName.value = FName; 36 if (FAction=="CopyFile") { 37 DName = prompt("CopyFile", FName); 38 top.hideform.FName.value += " "; 39 } else if (FAction=="MoveFile") { 40 DName = prompt("MoveFile", FName);</pre>

Değiştirilmiş Dosyayı Orijinal Olarak Kaydet Kapat

Aracı Listesi

İkon Liste Tümü Algılanan Araçlar Ayarlanmamış Araçlar Tüm Sunucular

WIN-1GC3MU...

Ready

WARSS İşlevleri

Yönetim Özellikleri

İşlev Adı	Açıklama
Güncelleme Yönetimi	Temsilci ve Yönetici güncellemeleri, sürüm yönetimi
İzinler ve Raporlama Yönetimi	<ul style="list-style-type: none">• Hesap ve kullanıcıya göre izin yönetimi• Harici sistemlerle arayüz oluşturma (ESM, SMS, E-posta, vb.)• Raporlar ve istatistikler
İstikrar	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Her kullanıcı hesabı için güvenli yükleme hedef dizinini belirtin• Güvenli Yükleyici kullanılarak yüklenen dosyalarda kötü amaçlı kod olup olmadığını da kontrol edin

Yönetim Görünümü

Yönetici İzinleri

Admini Yönet

WARSS (192.168.1.49)

Admin Listesi >

Admin Yetkisi >

Aracı Yetkisi (Admin) >

Aracı Yetkilisi (Aracı) >

Özellikleri Yükle >

Mesaj ayarları >

Yetkiler

Yetki Düzeyi	Süper Yönetici Yetki
<input type="checkbox"/> Süper Yönetici	<input checked="" type="checkbox"/> Aracı - Algılama İşlevi
<input type="checkbox"/> Orta Düzey Yönetici	<input checked="" type="checkbox"/> Aracı - Ayarlar (Genel, WAS)
<input type="checkbox"/> Genel Yönetici	<input checked="" type="checkbox"/> Aracı - Ayarlar (Algılama Kuralları)
<input type="checkbox"/> Kontrol Operatörü - Çoklu	<input checked="" type="checkbox"/> Aracı - Duraklat/Yeniden Başlat
<input type="checkbox"/> Kontrol Operatörü - Tek	<input checked="" type="checkbox"/> Sunucu - Çoklu Sunucuyu Kullan
	<input type="checkbox"/> Sunucu - Ayarlar
	<input type="checkbox"/> Admin Oluştur
	<input type="checkbox"/> Aracı Atama, Grup Oluştur
	<input type="checkbox"/> Dosya yükle
	<input type="checkbox"/> Mesaj ayarları
	<input type="checkbox"/> Aracıyı Sil

Ekle Sil

Uygula

Yönetim Görünümü

İstikrar



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 aşırsa uyarı ver %
- Sistem CPU Kullanımı %

- Duraklama Döngüsü :

Güncelleme Ayarları

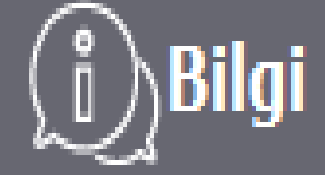
- Java güncellemesi : Etkin

Log Ayarları

- Log Yedekleme Döngüsü :
- Log Temizleme Döngüsü : geçmiş Saat de dakika
- Log Temizleme Ayarları : Zamana Dayalı Log Otomatik Temizleme Gün
- Kapasiteye Dayalı Log Otomatik Temizleme Mbyte(s)

Yönetim Görünümü

Kaynak Durumu İzleme



Bilgi

WARSS > IIS > (6)WIN-1GC3MUENMTA

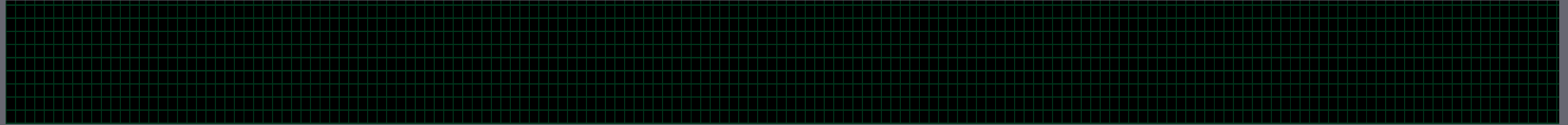
Aracı Bilgileri | Sistem Bilgisi | **Kaynak Durumu**

Aracı CPU Kullanımı



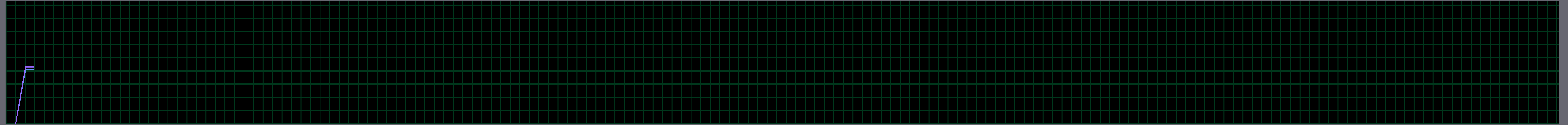
Aracı CPU Kullanımı : 0.0%

Sistem CPU Kullanımı



Sistem CPU Kullanımı : 0.0%

Hafıza



Fiziksel Bellek

› Kullanım Oranı : 44.9%
› Toplam : 2047.4MB
› Kullanılmış : 919.3MB
› Mevcut : 1128.1MB

Sanal Bellek

› Kullanım Oranı : 47.3%
› Toplam : 41.4MB
› Kullanılmış : 19.6MB
› Mevcut : 21.8MB

Hard Disk

› Kullanım Oranı : 54.0%
› Toplam : 19.6GB
› Kullanılmış : 10.6GB
› Mevcut : 9.0GB

Yönetim Görünümü

Saldırgan IP Tespiti

Saldırgan IP Algılama ☐ ✕

· Erişim Log Listesi (0 Öğeler)

WAS	Log Erişim Yolu	Yapılandırma Dosyası
-----	-----------------	----------------------

◀ | | ▶

(0 Öğeler)

Durum	Dosya
-------	-------

Sil Uygula Kapat

Yönetim Görünümü

Tercih Yönetimi

Ayarlar WARSS > IIS > (6)WIN-1GC3MUEMNTA

Genel | WAS | **Dosya Algılama** | Gelişmiş

Temel Algılama Ayarları Genel

Gerçek zamanlı Gözetim : Etkin

Çalıştırma Döngüsü : **Yok**

Yeniden tara : Etkin CPU Kullanım Limiti : 10

Min. Sahtecilik Dosya Boyutu : **0** Byte Sahtecilik Onar : Etkin

Yedekleme Dosya Numarası : **2** Öğeler Algılama dosya sayısı aşıldığında bildirim gönder : **0** Öğeler

Temizleme Ayarlarını Yedekle : Zamana Dayalı Yedekleme Otomatik Temizleme **90** Gün

Uzantı Baypaslarını Algıla : Etkin

Algılanan dosyaların son kontrol edilmesinden bu yana geçen süre aşıldığında bildirim gönder : **10** Saat

Sahtecilik Dosya Boyutunu Sınırla : **5120** KByte(s) Toplam Bellek Kullanımı %95'i Aştığında Duraklat : Etkin

Algılama Dizin Ayarları (1 Öğeler)

Etkin	Dizin	Durum	İçin	Yazılabilir	Ayarlar	Kod	Sahtecilik	İ Yükle	Uzantılar	URL	Log Yol Bilgileri

Yönetim Görünümü

Özel Güvenli Yükleyici

Dosya Yüklemelerini Yönet

WARSS (192.168.1.47)

Aracı Listesi

3 Katmanlı 2 Katmanlı

Tümü

- Apache
- Gruplanmamış
- IIS
- (6) WIN-1GC3MUENMTA [Bağlan](#)

Kullanıcı yol izinleri düzenle [Kurtarma için Ayarla](#) [Kurtarmadan Kaldır](#)

Sınıf	Path
-------	------

Yükleme Hedefi

- C:
- \$Recycle.Bin
- \$SysReset
- \$WINDOWS.~BT
- \$Windows.~WS
- .GamingRoot
- Boot
- Config.Msi
- Documents and Settings
- DumpStack.log
- DumpStack.log.tmp
- hiberfil.sys
- Intel
- OEM
- OneDriveTemp
- pagefile.sys
- PerfLogs

Path :

[Ayarlar](#) [Sil](#) [Uygula](#)

WARSS İşlevleri

Bulut Bilişim Desteği

İşlev Adı	Açıklama
Ölçek Giriş/Çıkış	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

Çalıştırma Döngüsü : Yok

Yeniden tara : Etkin CPU Kullanım Limiti : 10

Min. Sahtecilik Dosya Boyutu : 0 Byte Sahtecilik Onar : Etkin

Yedekleme Dosya Numarası : 2 Öğeler Algilama dosya sayısı aşıldığında bildirim gönder : 0 Öğeler

Temizleme Ayarlarını Yedekle : Zamana Dayalı Yedekleme Otomatik Temizleme 90 Gün

Uzantı Baypaslarını Algıla

Algılanan dosyaların son kontrol edilmesinden bu yana geçen süre

Sahtecilik Dosya Boyutunu Sınırla

Algilama Dizin Ayarları

Etkin	Dizin
-------	-------

Sahteciliğe Karşı Algilama Dizin Ayarları - WIN-1GC3MUEMNTA(192.168.1.43)

Sahtecilik Önlemeyi Algilamae Dahil Et Kurtarmadan hariç tut (0 Öğeler) Etkin

Path

Dizin Ayarları Sil Uygula

Log Yol Bilgileri

(1 Öğeler)

Dizin Ayarları WAS Dizin Sil

Reset Sahteciliğe Karşı Algilama Dizin Ayarları Uygula

Bulut Ayarları Görünümü

Kayıt/Tarih Yönetimi

Gözetim 🔍 ✕

Sahtecilik Tespiti Uyarılar Aracı Durumu
 Algılama Hataları Ağ durumu

Bugün Süre Belirt

31.12.2024 ~ 31.12.2024 Ara

İçindekiler	Aracı Adı	Sunucu Adı
Ağ bağlantısı kesildi.	(5) localhost.locald...	WARSS
Sahtecilik geri yükle dosyası geri yüklendi.	(6) WIN-1GC3MUE...	WARSS
Ayarlar dosyası değiştirildi.	(6) WIN-1GC3MUE...	WARSS
Ağa bağlandı.	(6) WIN-1GC3MUE...	WARSS
Aracı silindi.	(4) WIN-1GC3MUE...	WARSS
Sahtecilik geri yükle dosyası geri yüklendi.	(5) localhost.locald...	WARSS
Ayarlar dosyası değiştirildi.	(5) localhost.locald...	WARSS
Ayarlar dosyası değiştirildi.	(5) localhost.locald...	WARSS
Aracı algılanmayacak şekilde ayarlanmıştır.	(5) localhost.locald...	WARSS
Ayarlar dosyası değiştirildi.	(5) localhost.locald...	WARSS
Aracı algılanmayacak şekilde ayarlanmıştır.	(5) localhost.locald...	WARSS
Ayarlar dosyası değiştirildi.	(5) localhost.locald...	WARSS
Ağa bağlandı.	(5) localhost.locald...	WARSS
Sahtecilik önleme dosyası algılandı.	(4) WIN-1GC3MUE...	WARSS
Ayarlar dosyası değiştirildi.	(4) WIN-1GC3MUE...	WARSS
Aracı algılanmayacak şekilde ayarlanmıştır.	(4) WIN-1GC3MUE...	WARSS
Ayarlar dosyası değiştirildi.	(4) WIN-1GC3MUE...	WARSS
Aracı silindi.	(3) WIN-1GC3MUE...	WARSS
Aracı silindi.	(2) WIN-1GC3MUE...	WARSS
Ağa bağlandı.	(4) WIN-1GC3MUE...	WARSS

WARSS Şirket İçi Yapılandırma Şeması

