



WARSS

Website Attack Restoration Security Solution

Real-time website security



Contents

01

About Us

02

**Trends in Web
Hacking**

03

The Problem

04

WARSS

05

Use Cases

06

Q&A

umv



UMV Inc.

Founded in 2008

Seoul, South Korea

Web-Focused Solutions

Real-time web server security

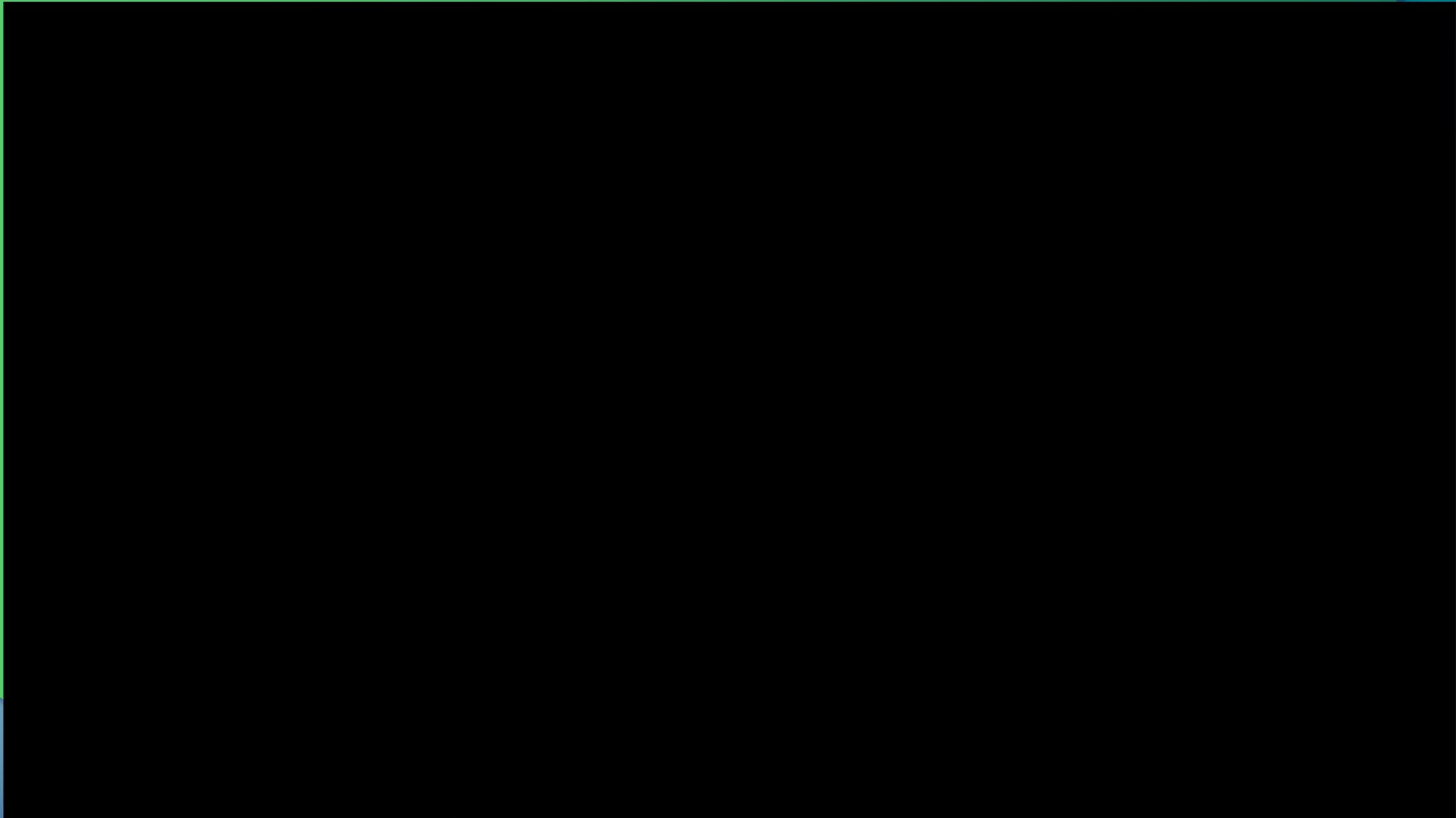
Prevent

Stolen data, interrupted web services,
website defacement, persistent attacks

Motto

“The security chain is only as strong as its
weakest link”

Why WARSS?



<https://www.youtube.com/watch?v=6gY1NWw9CJA&t=12s>

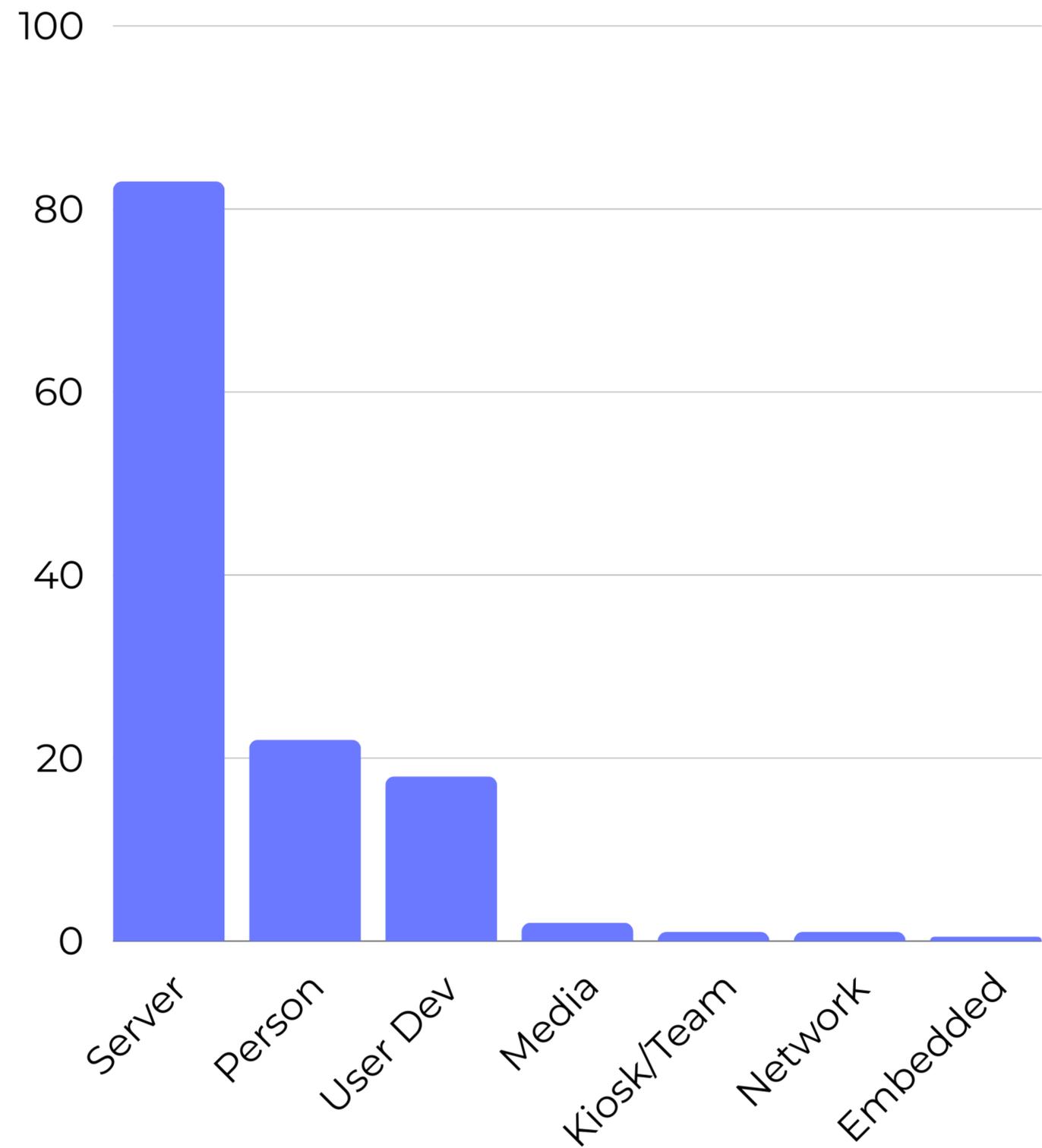
Web Hacking on the Rise

Verizon analyzed a record-high **TWO-FOLD** increase in the number of verified **security breaches** between 2022-2023

2024 Verizon Data Breach Investigations Report

Assets affected in breaches

2023 Verizon DBIR



Ukrainian & Russian Websites Defaced

Fake News

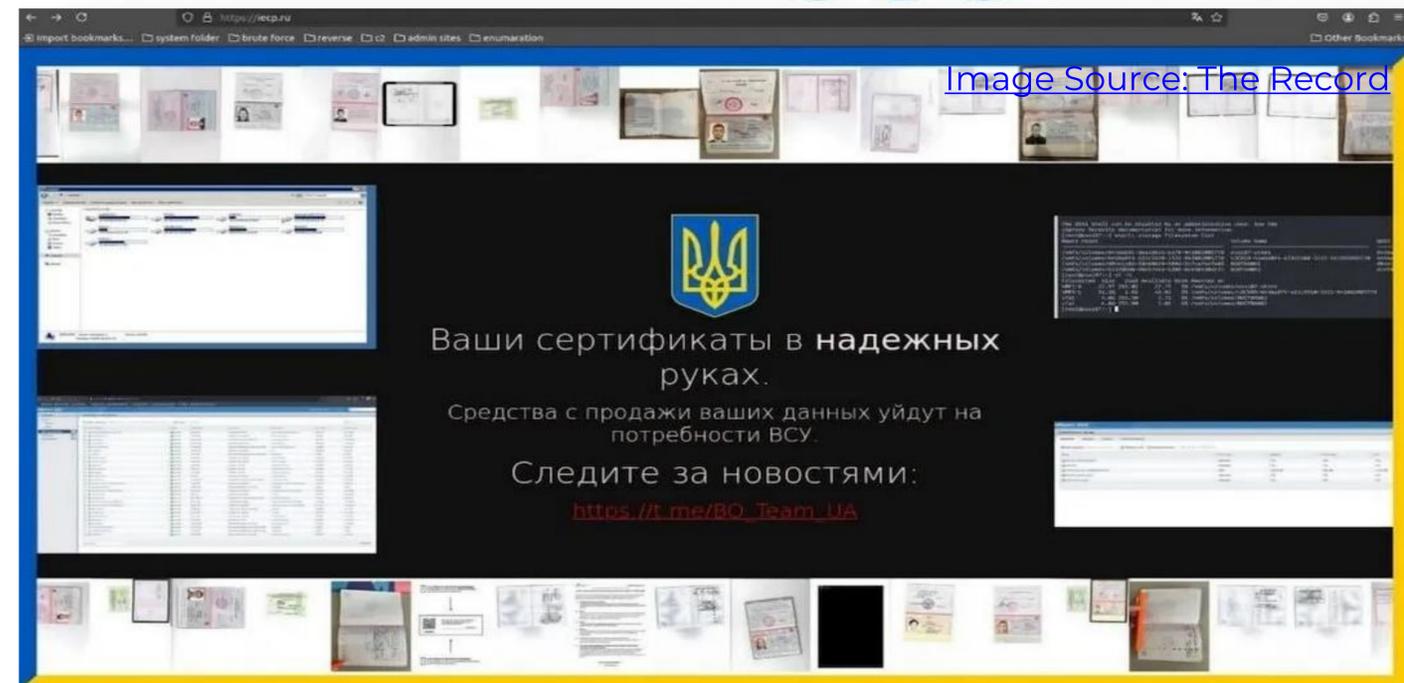
Feb. 2024-Present: Russo-Ukrainian War accompanied by continuous cyber attacks on one another and allies

Misinformation & Data Harvesting

Targets include SMBs, media outlets, government institutions, OT, and other entities possessing personal/sensitive information

Distrust: The Key to Cyberwarfare

Publicizing hacking attacks breeds fear, distrust of authorities, and misinformation amongst civilians



Internet Archive Attacks

Round 1: DDoS, Defacement, Data Theft

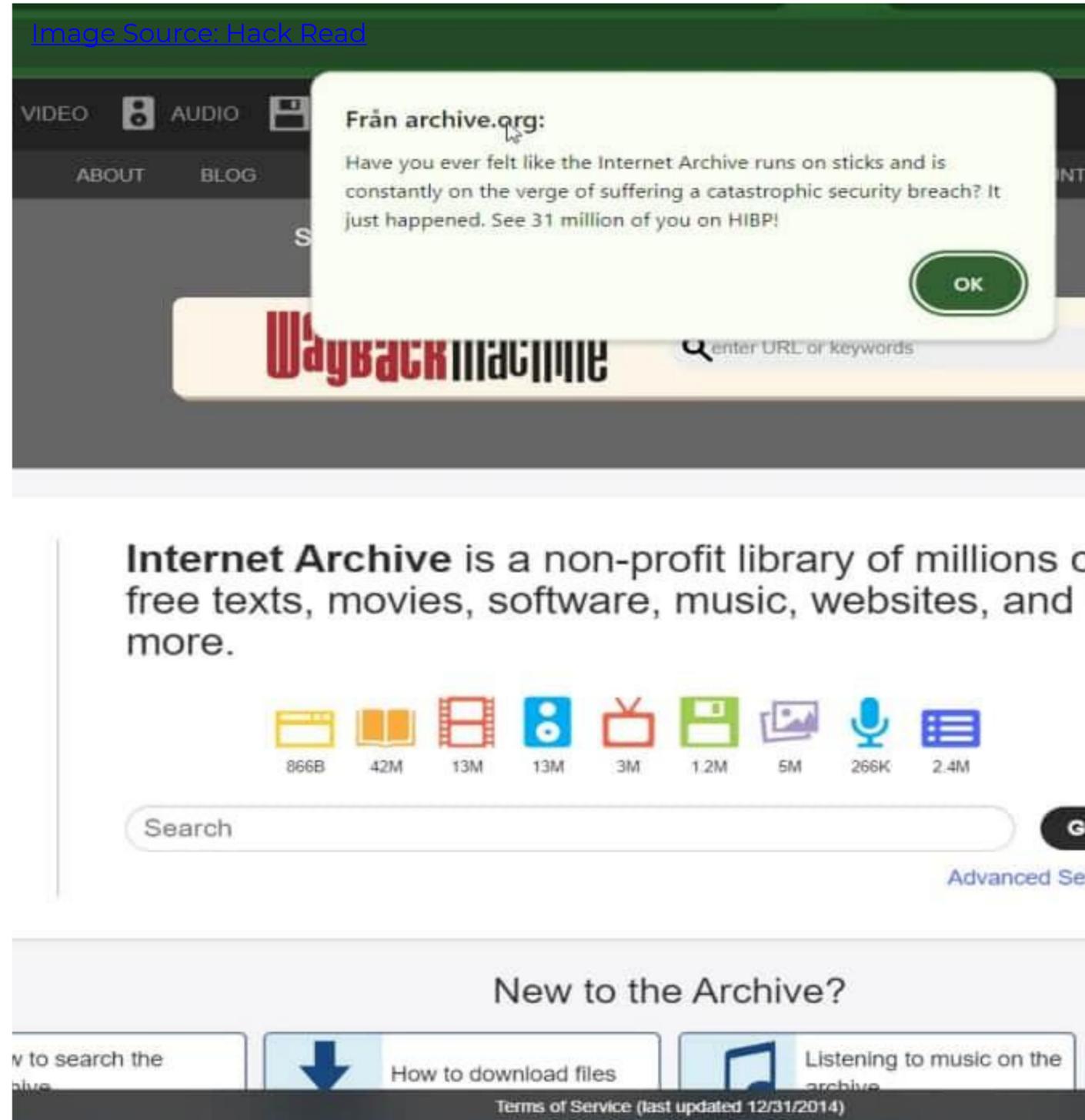
Oct 9, 2024: DDoS attack takes down site; website **defaced with JavaScript** alert; usernames, emails, etc. for **31 million user** accounts leaked

Back to Normal

Oct 18, 2024: IA confirms that data is safe and services restored

Round 2: Unsecured Digital Keys

Oct 20, 2024: Exploit unrotated access tokens to gain access to Internet Archive's Zendesk support platform; accessed **800K+ support tickets** going back to **2018**



- <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: Hacktivism and Cyber Terrorism

- Hacking to promote **political** or **religious** beliefs
- Increased availability of **encrypted communication platforms** (i.e. Telegram, Rocket Chat, Discord, etc.) and **cryptocurrency**
 - **TRON** accounted for **~90% of funds** associated with **terrorist financing** since 2021 (INTERPOL New Technologies Forum, October 2023, Merkle Science)
- **Cybercrime-as-a-service** (DDoS, ransomware, credentials, data, etc.)

- *Beneath the Surface Report* (June, 2024)
UN Counter-Terrorism Centre (UNCCT)



[Image Source: Malcontent News](#)



[Image Source: POLITICO](#)

The Problem

Defacement Methods

1. Source Code Modification

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
iform to Mt Gox. Anybody interested? < 1	4xCoder	24	1564	Today at 07:32:20 pm by AlexZ
	mizerydeana	17	562	Today at 07:19:34 pm by ssaCEO
pydun buttc01s.org		17	1501	Today at 06:58:32 pm by enmakou

Image Source: alphavilleherald.com



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!

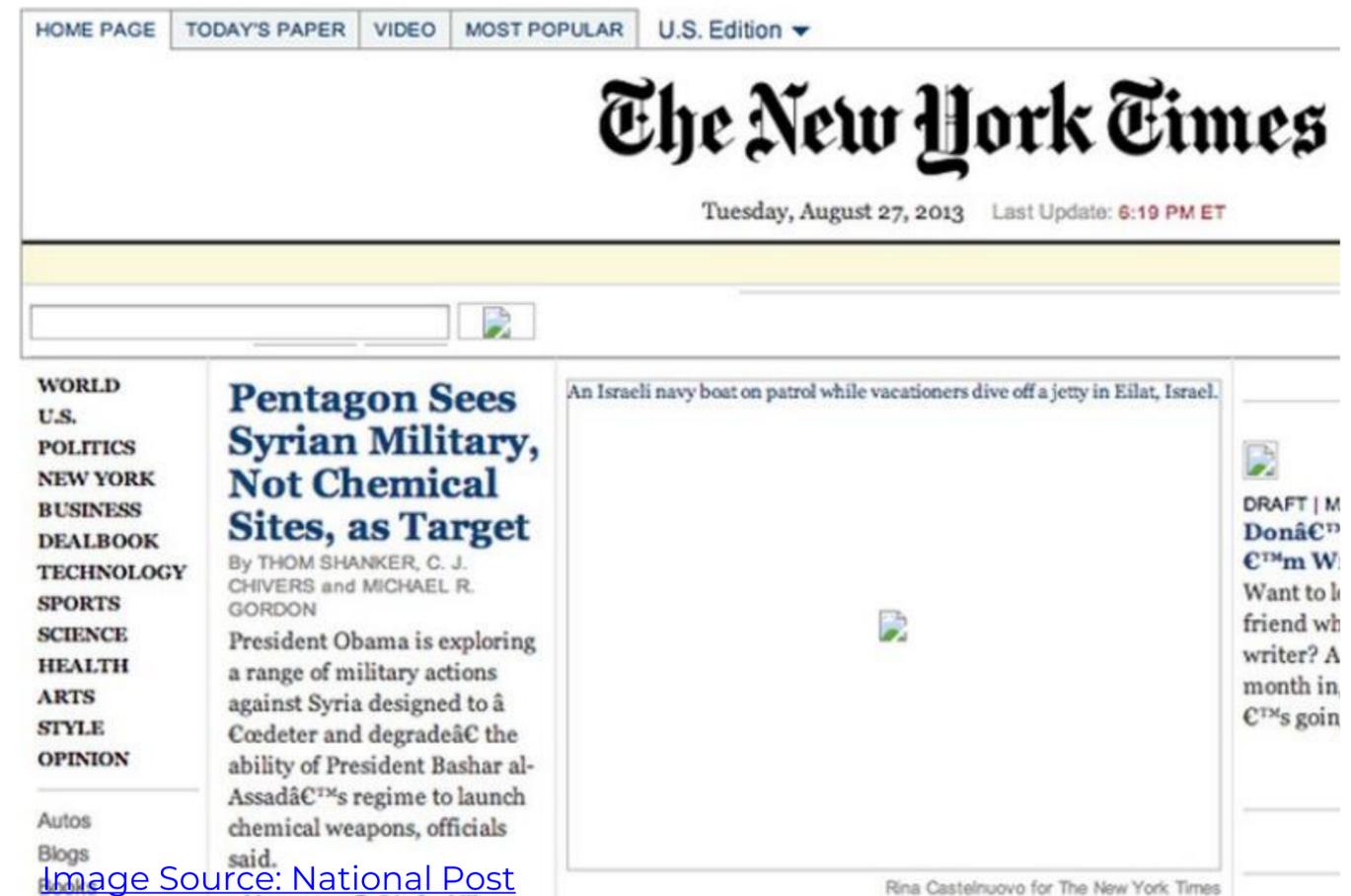
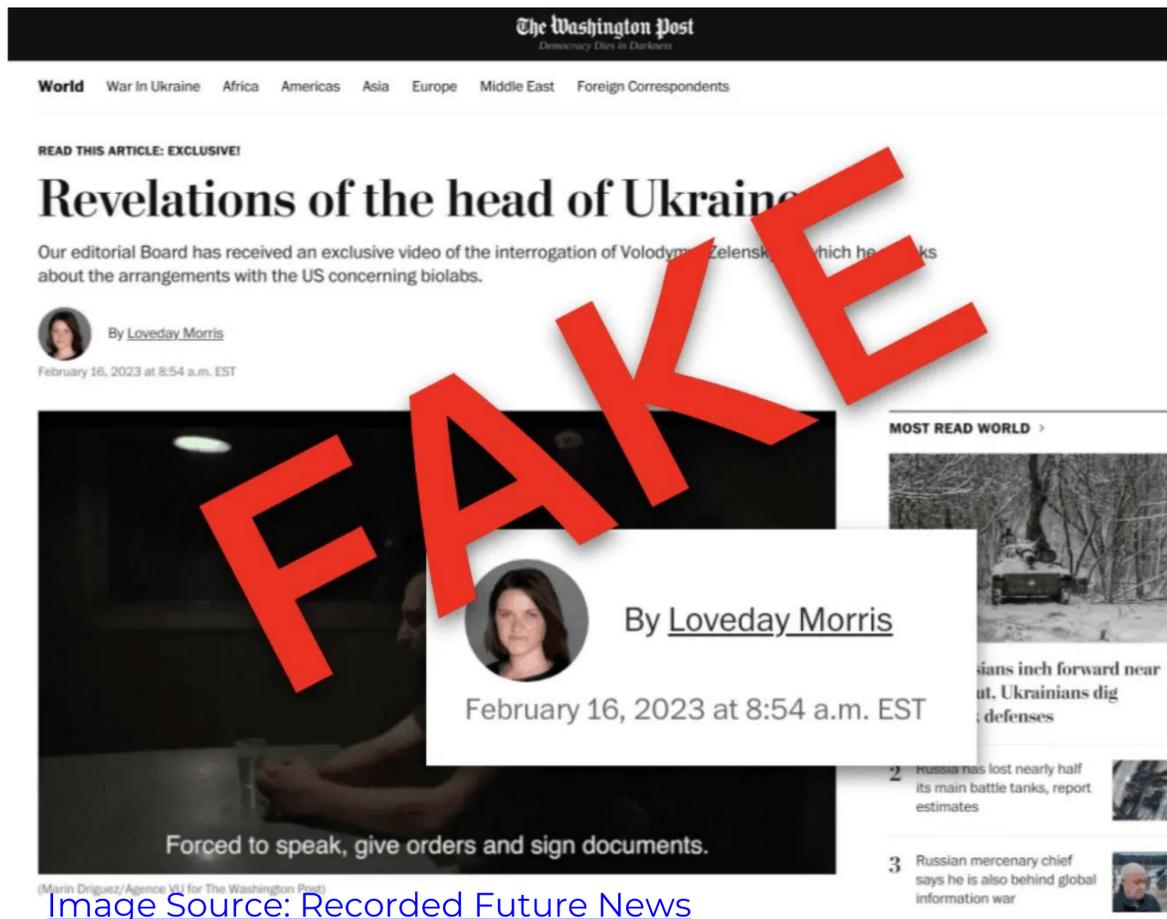
犯我中华者虽远必诛!

Py. China Hack **보안뉴스** Intelligence Bureau

Image Source: boannews.com

Defacement Methods

2. Content Spoofing/Injection



Why Defacement?



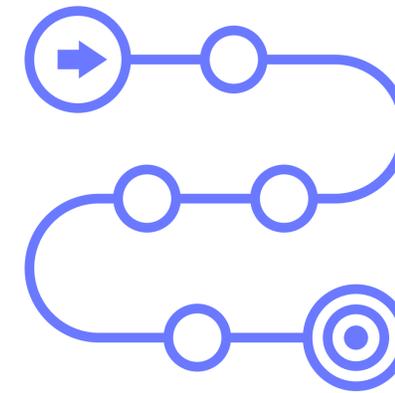
Motivation

- hacktivism
- embarrassment
- fame/recognition
- cyber terrorism



Target

- government institutions
- healthcare
- large companies
- targets of convenience

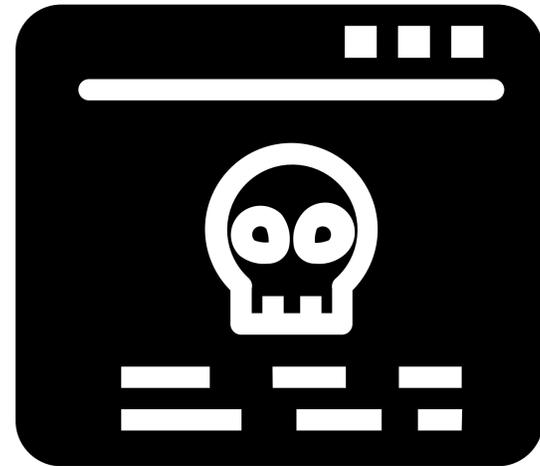
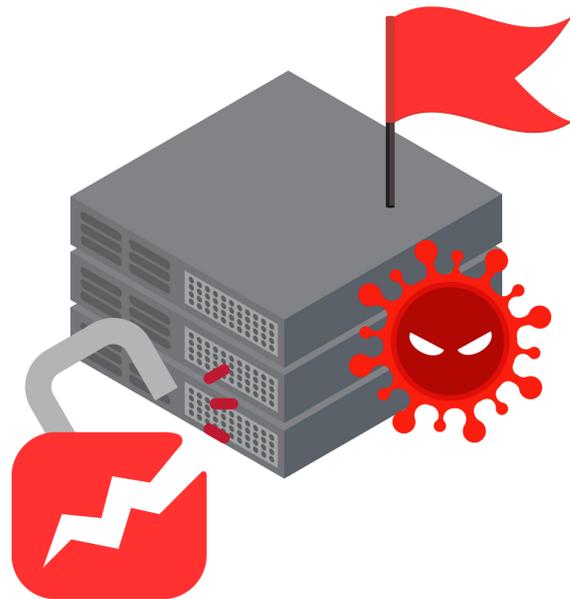


Method

Exploit weaknesses in web-based components:

- web server
- web applications
- websites

The Anatomy of a Web Attack



3

Impact

- Defacement
- Source code and content forgery

2

Escalation

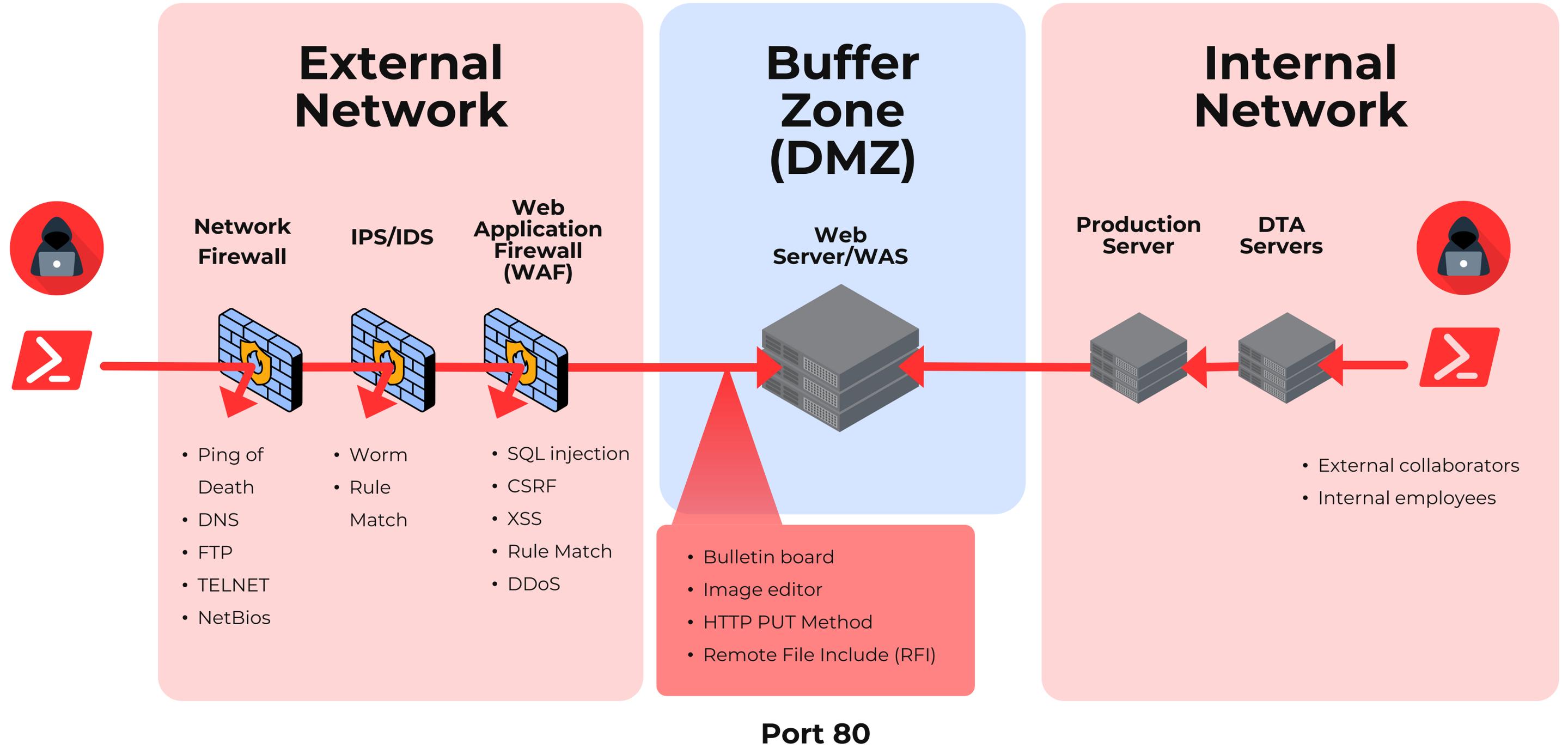
- Malware uploaded on web server to establish presence
- Additional malware (payload) executed to change web server files

1

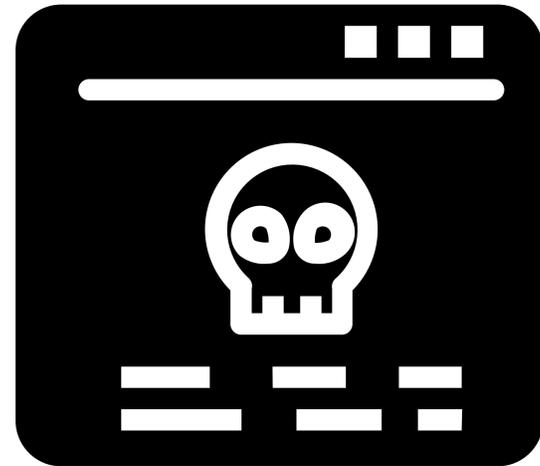
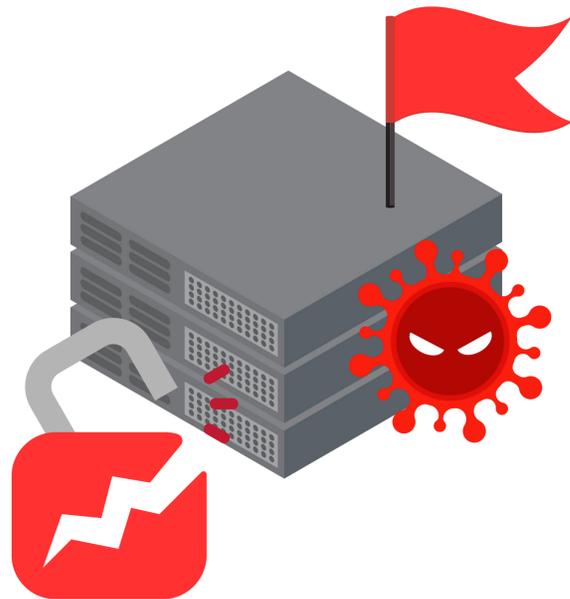
Infiltration

- Web server or WAS vulnerabilities exploited to gain initial access
- E.g. SQL injection, stolen credentials, phishing

The Status Quo



The Anatomy of a Web Attack



3

Impact

- Defacement
- Source code and content forgery

2

Escalation

- Malware uploaded on web server to **establish presence**
- Additional malware (payload) executed to change web server configuration files

1

Infiltration

- Web server or WAS vulnerabilities exploited to gain initial access
- E.g. SQL injection, stolen credentials, phishing



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

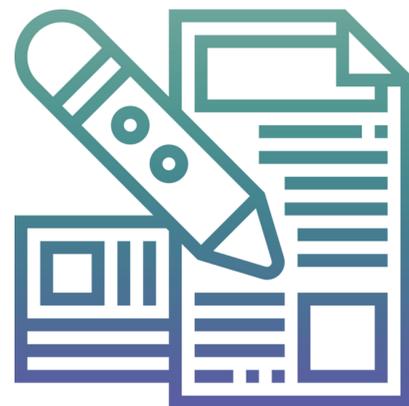
<https://blog.sucuri.net/wp-content/uploads/2023/03/image-1.jpg>

The Key: Real-time Detection & Response

All attacks start with one of three **changes**:



1
File Addition



2
File Modification



3
File Removal

Website Attack Restoration & Security Solution (WARSS)

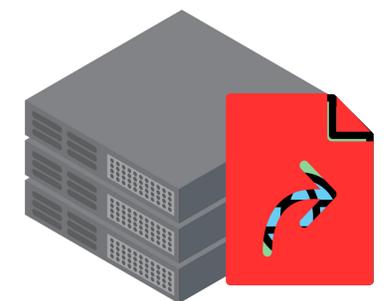
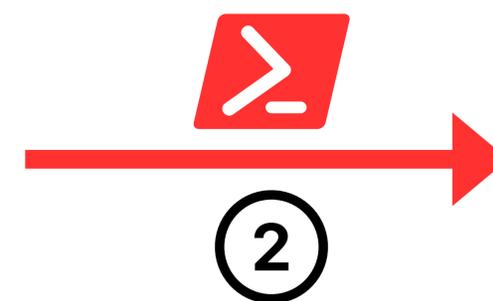
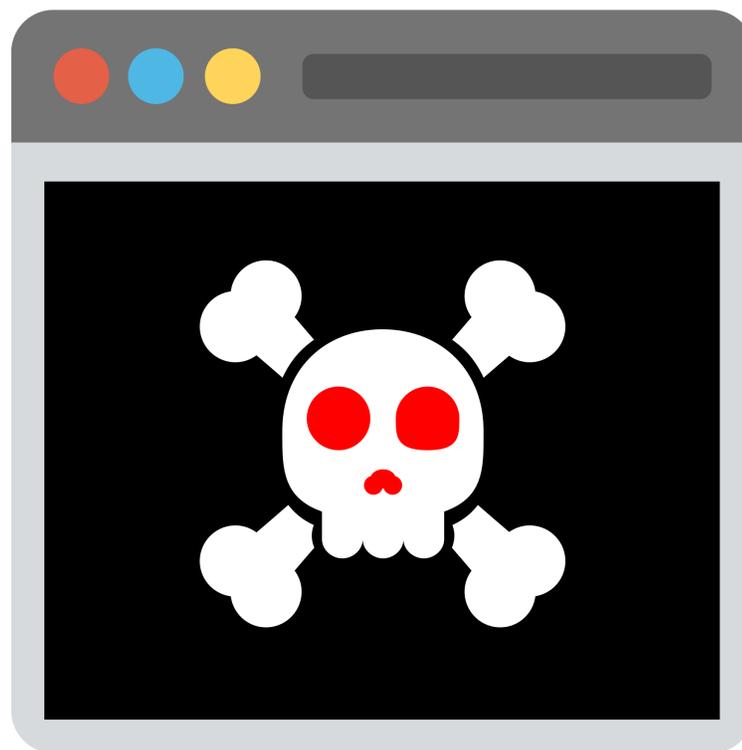
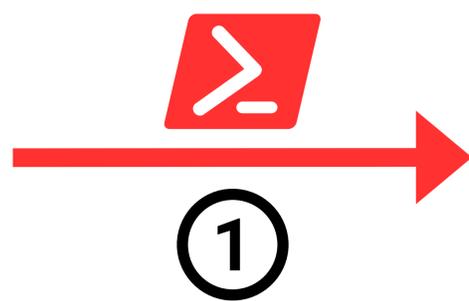
Web server security booster solution that **detects** unauthorized changes to a website and **restores** the original files in **real-time**



How Does Website Defacement Happen?

vulnerable website

web server



How Does WARSS Work?



Demo

The screenshot displays the WARSS 2.7.0.4 interface. The main terminal window 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 Monitor panel on the right shows the following settings and logs:

- Anti-Falsification Detection:
- Detection Errors:
- Warnings:
- Network Status:
- Agent Status:

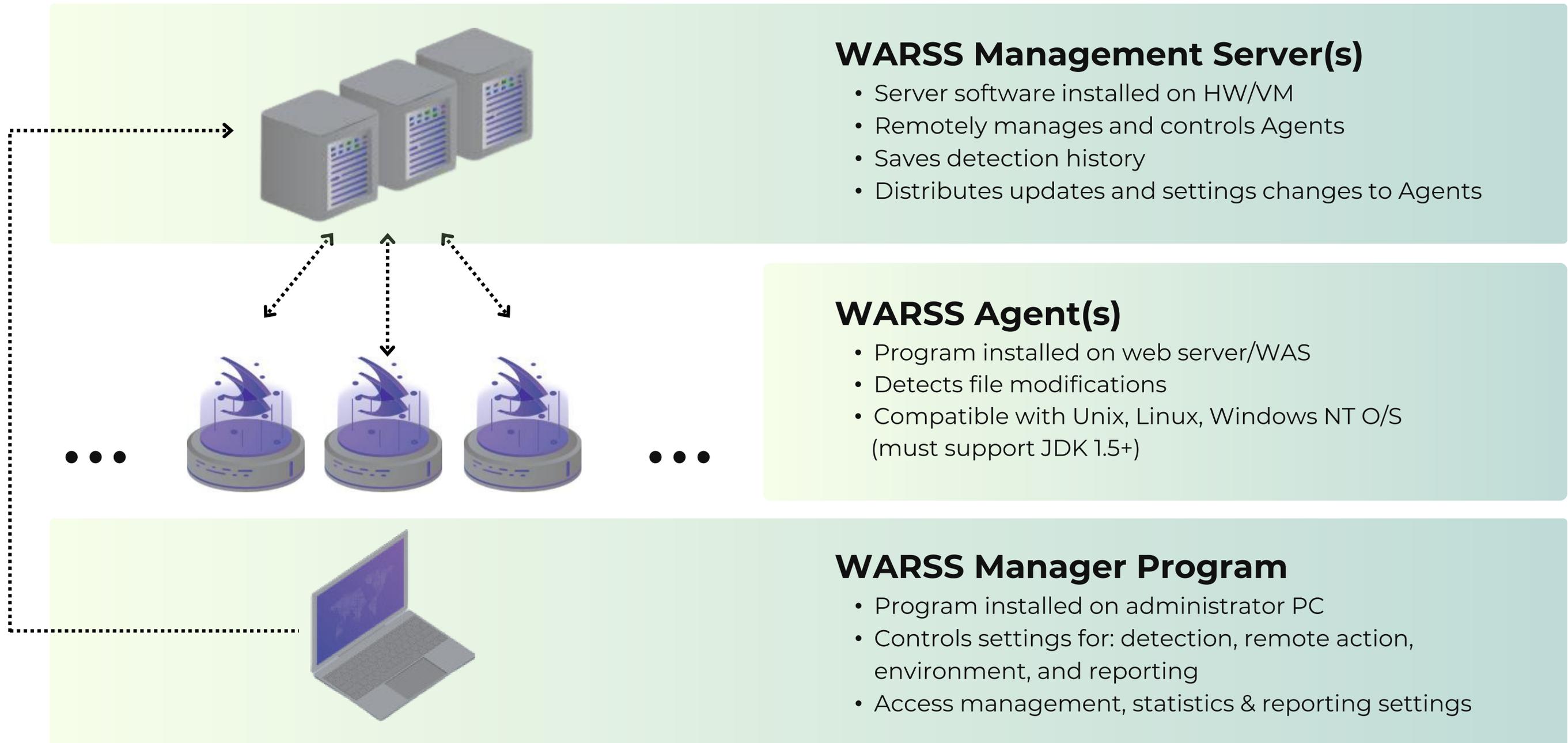
Search filters: Today, Specify Period (25.06.2024 ~ 25.06.2024), Search

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
Agent set not to detect.	(1) localhost.locald...	WARSS
Network connected.	(1) localhost.locald...	WARSS

Agent List panel shows: Icon, List, All, Detected Agents, Unset Agents, All Servers. A single agent is listed as localhost.local...

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

WARSS Configuration



WARSS Management Server(s)

- Server software installed on HW/VM
- Remotely manages and controls Agents
- Saves detection history
- Distributes updates and settings changes to Agents

WARSS Agent(s)

- Program installed on web server/WAS
- Detects file modifications
- Compatible with Unix, Linux, Windows NT O/S (must support JDK 1.5+)

WARSS Manager Program

- Program installed on administrator PC
- Controls settings for: detection, remote action, environment, and reporting
- Access management, statistics & reporting settings

How WARSS is Different

WARSS



Web Crawlers



Detection Method:

Real-time, pattern-based

Periodic detection

Load:

Optimized resource usage (~1% CPU)

Agentless

Detection Target:

Server files (source code, data, contents)

Compiled URL units and **data files**

Mitigation:

Real-time, automatic restoration

Manual mitigation upon breach

Real-time
detection

Protect
source code
and contents



Lightweight

Immediate
restoration & recovery

ZERO TRUST

1. “Never trust, always verify”
2. Least-privilege access
3. Assume breach

ZERO TRUST

3. Assume breach



**Real-time
detection**

**Streamlined
management**

**Rapid
mitigation**

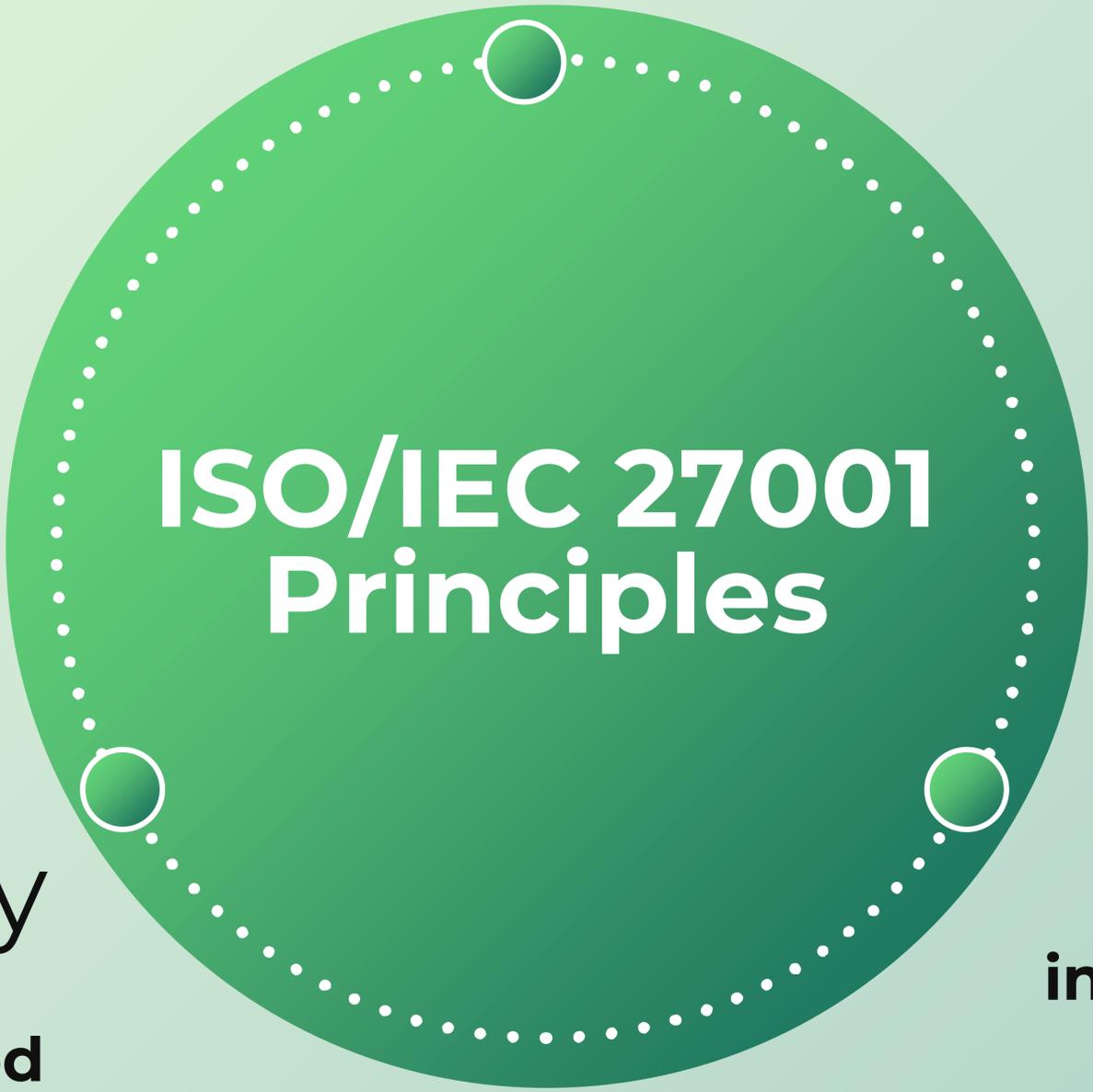
**Real-time file
change monitoring**

**Real-time alerts
and reports**

**Automated
restoration &
recovery**



Availability
information is accessible
when needed



Confidentiality
information only
accessible to authorized
parties



Integrity
information is accurate
and protected from
corruption

ISO/IEC 27001 Compliance

Applicable Requirements:

- 8.1** Operational planning and control
- 8.3** Information security risk treatment
- 9.1** Monitoring, measurement, analysis and evaluation



ISO/IEC 27001 Compliance

Applicable Annex A Technological Controls:

- 8.4** Access to source code
- 8.6** Capacity management
- 8.7** Protection against malware
- 8.8** Management of technical vulnerabilities
- 8.12** Data leakage prevention
- 8.13** Information backup
- 8.15** Logging
- 8.16** Monitoring activities
- 8.23** Web filtering
- 8.26** Application security requirements



GS (Good Software) Level 1 Certified

- **Test Standards:**
ISO/IEC 25023, 25051, 2504
- **Tested for:**
 - Functional suitability
 - Performance efficiency
 - Compatibility
 - Usability
 - Reliability
 - Security
 - Maintenance
 - Portability



Use Cases

Government Defense Institution

Security Shortfalls

Dissatisfied with “W” web-based forgery detection software’s performance and ease of management

Their Checklist

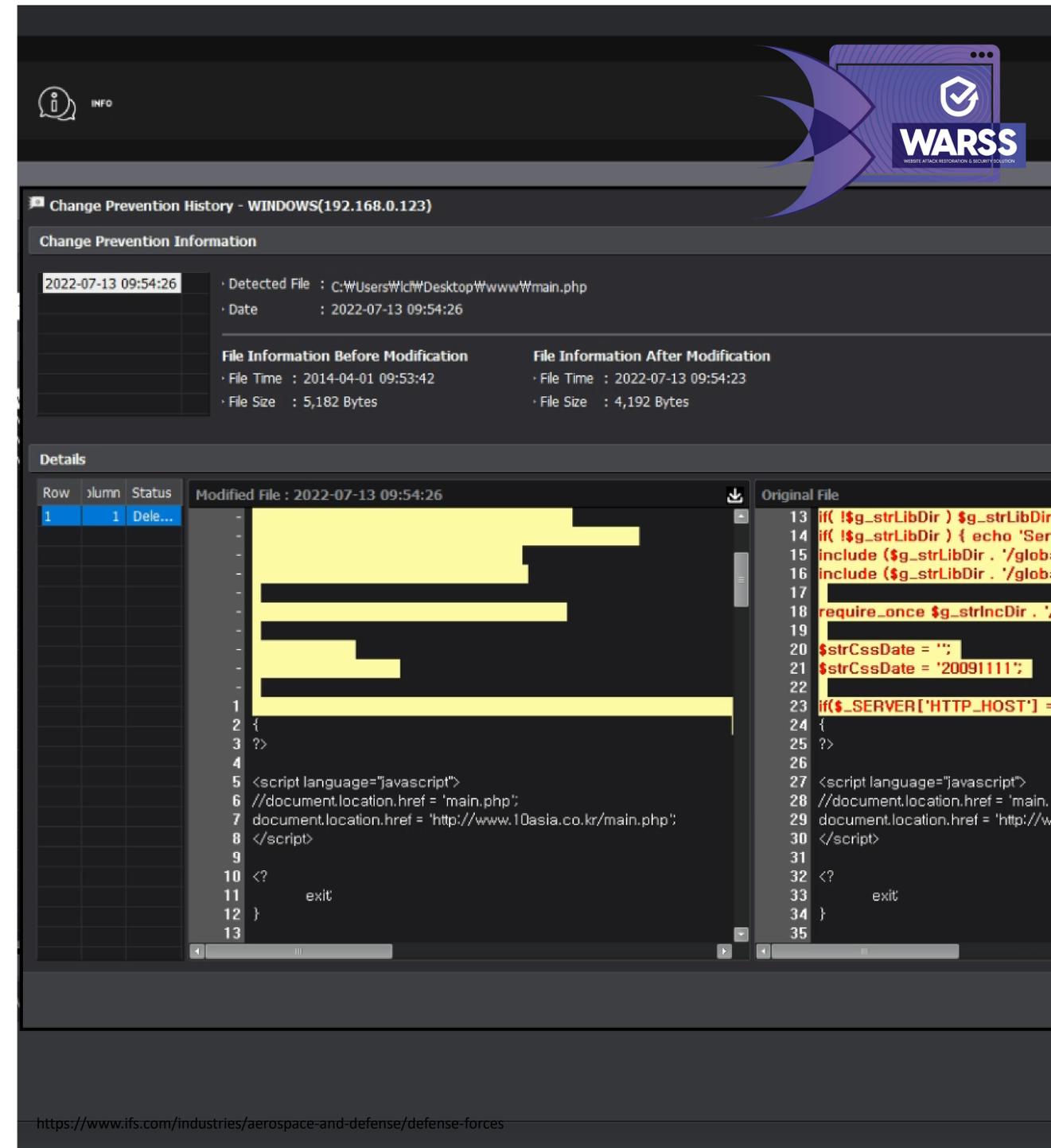
Were specifically looking for an Agent-based solution that offered automatic restoration and efficient management

2023 WARSS Implementation

Installed 50 WARSS Agents on all web servers

Their Feedback

Delighted with WARSS’s automatic home directory detection feature, allowing for easy detection configuration without manually inputting URLs



Transportation Agency

Content Forgery Concerns

Operating website with educational content (images, videos); tried and failed to outsource development of proprietary anti-forgery solution

Why WARSS?

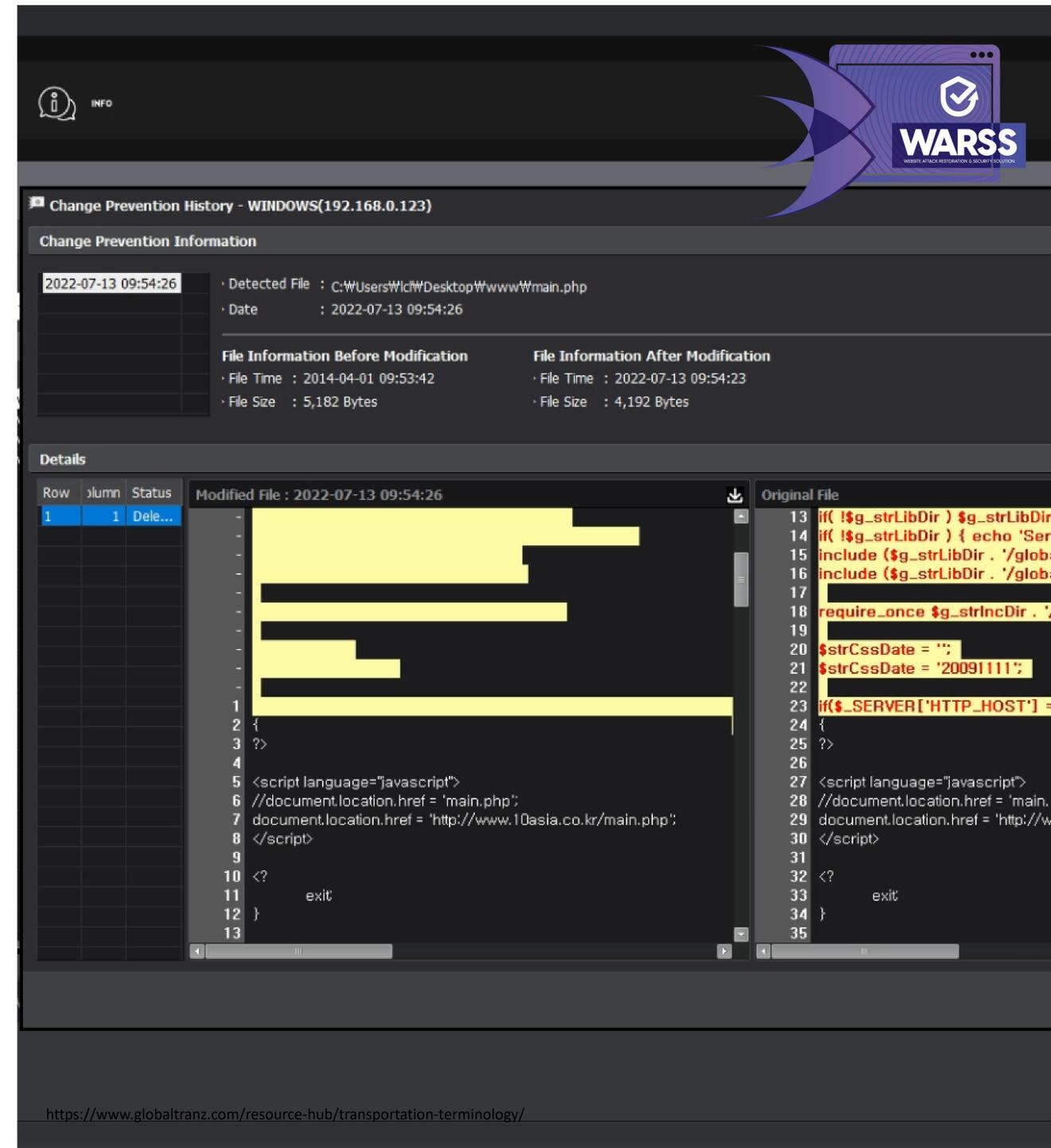
Compared to all other anti-forgery solutions they tested, WARSS was the only one that offered source code, image, and video forgery protection

Why They Chose WARSS

Installed 100 WARSS Agents on all web servers

Continuous Protection

WARSS has prevented any forgery incidents since; customer continues to purchase Agents each time they add servers to their system



Who Uses WARSS?

WARSS protects the reputations of several national companies and institutions.



... and more!

Hundreds of Customers

UMV products has been providing safe and stable protection for hundreds of customers' web servers for over a decade.



13+ years



13+



7-8



Hanwha

13+



10+



13+



TOYOTA



STARBUCKS



SUPREME COURT OF KOREA



Ministry of National Defense
Republic of Korea



HYUNDAI

Deloitte.

iMBC

... and many more!



Thank you

Contact Us

UMV, Inc.

Seoul, South Korea

 +82 2 448-3435

 sales@umvglobal.com

 www.umvglobal.com

Appendix

WARSS Functions

Forgery Detection and Restoration

Function Name	Description
Forgery Detection	Detection and notification of forgery and alteration of website source files and data
Forgery Restoration	Real-time restoration of original files when forgery is detected
Re-Assign Original	Re-assign baseline/original files when legitimate changes must be made

Forgery Detection View

Forgery Detection and Real-Time Restoration

The screenshot displays the WARSS 2.5.8 Anti-Forgery interface. The main window is titled "Anti-Forgery" and shows a list of detected files. A modal window titled "Change Prevention History - WINDOWS(192.168.0.123)" is open, displaying details for a file detected on 2022-07-13 at 09:54:26. The file path is C:\Users\Wlc\Desktop\www\main.php. The modal shows the file information before and after modification, and a comparison of the original and modified file contents.

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

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 = '/app/aknsys/phplib'; 14 if(!\$g_strLibDir) { echo 'Server Env Var not define'; exit(0 15 include (\$g_strLibDir . '/global_var.inc.php'); 16 include (\$g_strLibDir . '/global_func.inc.php'); 17 18 require_once \$g_strIncDir . '/10asia/lib/_VCONFIG.php'; 19 20 \$strCssDate = ''; 21 \$strCssDate = '20091111'; 22 23 if(\$_SERVER['HTTP_HOST'] == 'www.10-magazine.com' \$ 24 { 25 ?> 26 27 <script language="javascript"> 28 //document.location.href = 'main.php'; 29 document.location.href = 'http://www.10asia.co.kr/main.php'; 30 </script> 31 32 <? 33 exit 34 } 35</pre>

Buttons: Save Modified File as Original, Close

WARSS Functions

Management Features

Function Name	Description
Update Management	Agent & Manager updates, version management
Permissions and Reporting Management	<ul style="list-style-type: none">• Permissions management by account and user• Interfacing with external systems (ESM, SMS, E-mail, etc.)• Reports and statistics
Stability	<ul style="list-style-type: none">• Resources usage control• Customizations to suit server environment
Attacker IP Detection	Execution IP reports for forgery files (available when only detection function is activated)
Preferences Management	Web/WAS configuration file management and change detection settings
Dedicated Safe Uploader	<ul style="list-style-type: none">• Specify safe upload target directory for each user account• Check for presence of malicious code in files uploaded using Safe Uploader too

Management View

Administrator Permissions

Manage Admin □ ×

ShellMonitor-1 (192.168.0.119) ▼

- Administrator List >
- Admin Authority >**
- Agent Authority for Admin >
- Agent Authority for Agent >
- Upload Properties >
- Message Settings >

Authorizations

Authority Level	Authority
<input type="checkbox"/> 상급관리자	<input type="checkbox"/> Agent - Process Detections
<input type="checkbox"/> 중급관리자	<input type="checkbox"/> Agent - Settings (General, WAS)
<input type="checkbox"/> 일반관리자	<input type="checkbox"/> Agent - Settings (Detection Rules)
<input type="checkbox"/> 관제요원 - 멀티	<input type="checkbox"/> Agent - Pause/Restart
<input type="checkbox"/> 관제요원 - 싱글	<input type="checkbox"/> Agent - Update Pattern Manually
	<input type="checkbox"/> Server - Use Multi-Server
	<input type="checkbox"/> Server - Settings
	<input type="checkbox"/> Create Admin Account
	<input type="checkbox"/> Agent Allocation, Create Group
	<input type="checkbox"/> File Upload
	<input type="checkbox"/> Message Settings
	<input type="checkbox"/> Delete Agent

Management View

Stability

(1)localhost.localdomain ×

Settings ShellMonitor-1 > Unassigned > (1)localhost.localdo...

General | WAS | File Detection | Upload Filtering | Malicious URL List | Local Pattern List | Advanced

Server Access Settings View More

Web Server Safeguard Server Address : 192.168.0.122 Port : 7778
Upload Server Address : 192.168.0.122 Port : 7777
Detection File Management Server Address : Port : 0

General Settings

Detection Settings

CPU Usage Limit : 10
Issue alert if Agent CPU usage exceeds 50 %
System CPU Usage 0 %

Update Settings

Pattern Updates : Manual
 Automatic (Before Detecting)
 Periodic Every Day at 0 minute(s) past 0
 No full detecting when updating global pattern

Reset Apply

Management View

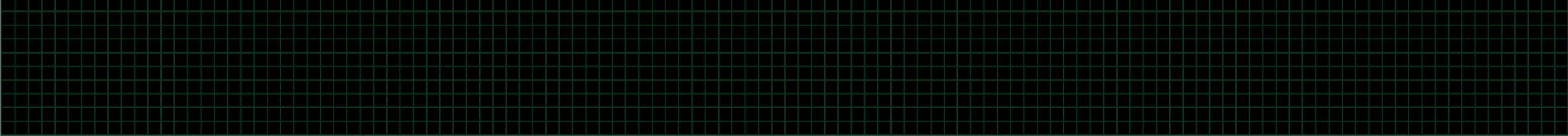
Resource Status Monitoring

(2)localhost.localdomain X

Information ShellMonitor-1 > Unassigned > (2)localhost.localdo...

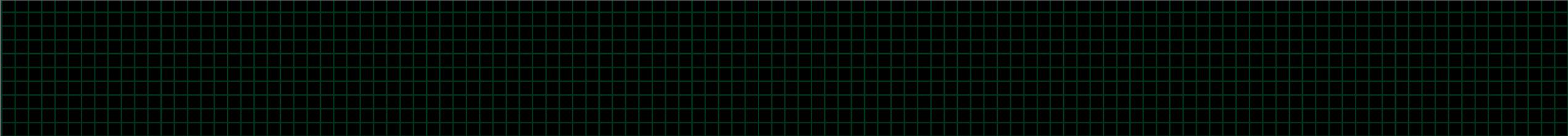
Agent Information | System Information | **Resource Status** | Docker Information | Docker Container Information

Agent CPU Usage



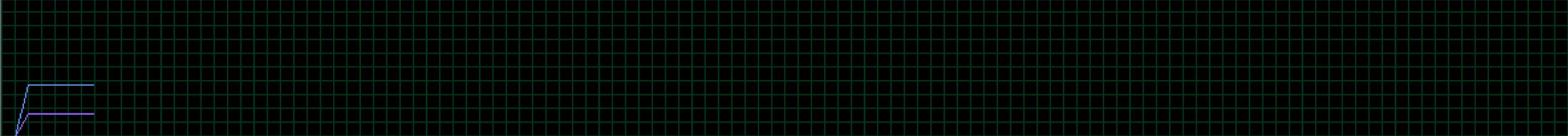
Agent CPU Usage : 0.0%

System CPU Usage



System CPU Usage : 0.2%

Memory



Physical Memory	Virtual Memory	Hard Disk
Usage Rate : 38.7%	Usage Rate : 17.9%	Usage Rate : 3.6%
Total : 3665.7MB	Total : 196.5MB	Total : 24.6GB
Used : 1420.5MB	Used : 35.3MB	Used : 0.9GB
Available : 2245.2MB	Available : 161.2MB	Available : 23.7GB

Management View

Attacker IP Detection

Attacker IP Detection ☐ ✕

Access Log List (Total 0)

WAS	Acces Log Path	Configuration File	Directory

Access Log List (Total 0)

Status	File

Delete Apply Close

Access Log List

Management View

Preferences Management

(2)localhost.localdomain x

Settings ShellMonitor-1 > Unassigned > (2)localhost.localdo...

General | WAS | **File Detection** | Upload Filtering | Malicious URL List | Local Pattern List | Advanced

Basic Detection Settings General

- Real-Time Monitoring : On
- Execution Cycle : **None** v
Rescan : On CPU Usage Limit : 10
- Forgery : Detection **0** Bytes Recover
- Malicious URL Detection : On Assign to White List for Full Detections
- Personal Information Detection : On (Social Security Number Alien Registration Number Individual Business Registration Number Mobile Phone Number Phone Number Account Number Card Number E-Mail Driver's License Number Health Insurance Number Passport Number)
- Countries subject to personal information detection : **Korea** v
- Backup Policy : Detected WebShells Detected WebShells & Changed Files Personal Information Detection File Backup
- No. of Backup Files : **2** v Send notification when number of detection files exceeds : **0** v
- BackUp Clearing Settings : Time-Based BackUp Auto-Clear **90** v Day(s)
- Automatic Quarantine : Well-Known WebShells Encoding Black List URLs Hash
- Detect Well-Known WebShells Only : On Detect Extension Bypasses : On
- Archive File Detection : On Send notification when elapsed time since detected files was last checked exceeds : **10** v Hour(s)
- Limit Detection File Size : **5120** v KByte(s) Pause When Total Memory Usage Exceeds 95% : On
- Limit Forgery File Size : **5120** v KByte(s) Hash Detection : On

Detection Directory Settings (Total 0)

On	Directory	Status	adabl	Writable	etting:	Code	Forgery	.ecove	Extensions	URL

Management View

Dedicated Safe Uploader

Manage File Uploads

ShellMonitor-1 (192.168.0.119)

Agent List

Removing Recovery

3-Tier 2-Tier

- All
 - Unassigned
 - (1) localhost.localdomain
 - (2) localhost.localdomain Connect ●

Upload Target

- C:
 - \$Recycle.Bin
 - \$WINRE_BACKUP_PARTITION.MARKER
 - %AMBU9P
 - @\$SDSEV
 - adobeTemp
 - Documents and Settings
 - DumpStack.log
 - DumpStack.log.tmp
 - for local
 - hiberfil.sys
 - pagefile.sys
 - Program Files
 - Program Files (x86)

Admin Edit Permission Paths	
Class	Path

Path :

Settings Delete Apply

WARSS Functions

Cloud Computing Support

Function Name	Description
ScaleIn/Out	<ul style="list-style-type: none">• Auto-registration of new detection targets on scale out; detection begins automatically• Automatic backups of detection/change/deletion logs to management server for deleted Agents on scale in
Home Directory Search	<ul style="list-style-type: none">• Schedule detections to find changes/additions to web/WAS home directory• View addition/change history of home directory
History Management	Agent operation status and history management (installation, deletion, start/stop, etc.)
Event Duplication Prevention	Prevent duplicate detection events from occurring in redundant systems when home directory is included in NAS area

Cloud Settings View

Home Directory Search

(2)localhost.localdomain X

Real-Time Monitoring : On
Execution Cycle : None
Rescan : On CPU Usage Limit : 10
Forgery : Detection Detect Recover
Malicious URL Detection
Personal Information Detection
Countries subject to personal info
Backup Policy
No. of Backup Files
BackUp Clearing Settings
Automatic Quarantine
Detect Well-Known WebShells On
Archive File Detection
Limit Detection File Size
Limit Forgery File Size

Detection Directory Settings

On	Directory

Anti-Forgery Detection Directory Settings - localhost.localdomain(192.168.0.119)

Include in Anti-Forgery Detection Exclude From Recovery (Total 0)

Path

Directory Settings Delete Apply

Hour(s) : 10

(Total 0)

IS	URL
----	-----

Directory Settings WAS Directory Delete

Reset Anti-Forgery Detection Directory Settings Apply

Cloud Settings View

Logging/History Management

The screenshot shows a 'Monitor' application window with the following settings and data:

- Anti-Falsification Detection
- Warnings
- Agent Status
- Detection Errors
- Network Status
- Today Specify Period
- Date range: 25.06.2024 ~ 25.06.2024
- Search button

Contents	Agent Name	Server Name
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
Network connected.	(1) localhost.locald...	WARSS

WARSS On-Premise Configuration Diagram

