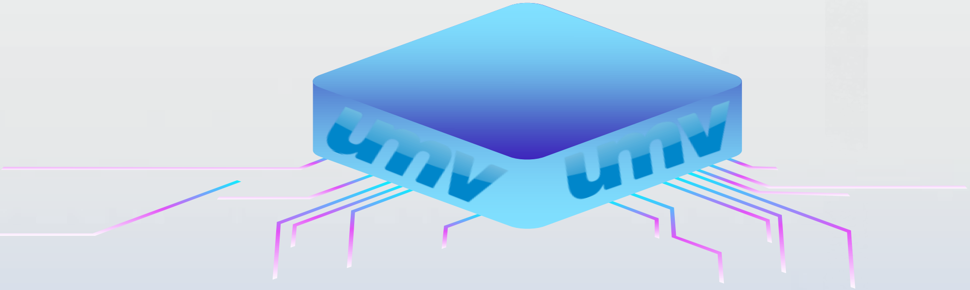
WEBSERVER SAFEGUARD

For web server & Cloud VM integrated security

WSS (Web Server Safeguard)

Complete web service security through real-time detection and isolation



▶ Watch Video

WSS
WEBSERVERSAFEGUARD
INFORMATION SECURITY WITH UNINTERRUPTED SERVICE
Webserver
Security Solution
On-Premise
Security booster solution for webservers, protecting information data and providing uninterrupted service
umv
WSS
INFORMATION SECURITY WITH UNINTERRUPTED SERVICE
WSS CLOUD
URITY WITH UNINTERRUPTED SERVICE
Webserver
Security Solution
CLOUD
Security booster solution for cloud computing (VM), protecting information data and providing uninterrupted service
WSS CLOUD
INFORMATION SECURITY WITH UNINTERRUPTED SERVICE

CONTENT

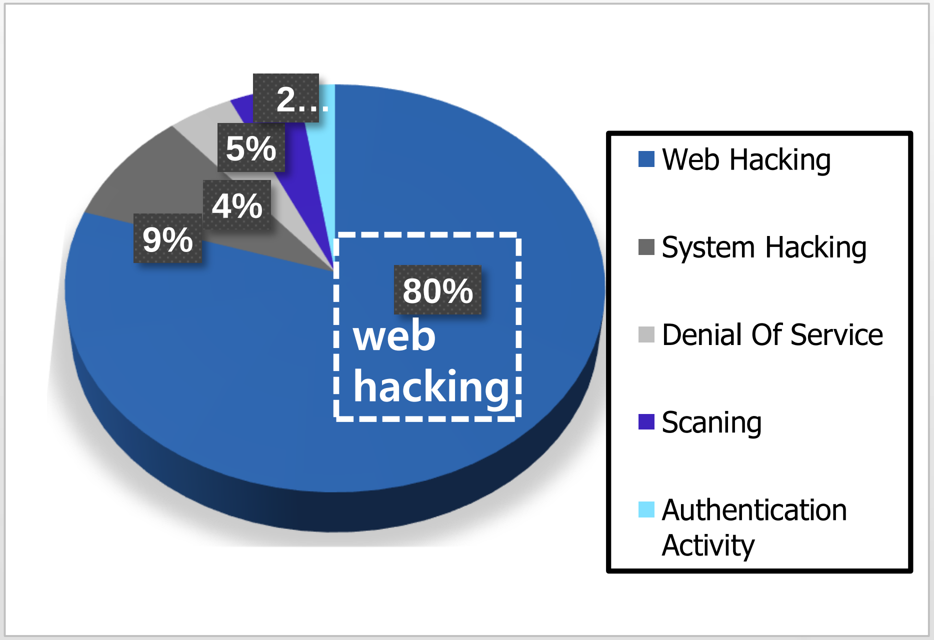
1. **Web security overview and necessity**
2. Introduction to WSS (overview and structure)
3. WSS main features
4. WSS main function

1. Web security overview and necessity

Worldwide, more than 80% of cyber attacks are carried out through web service servers, and the importance of web service security is increasing day by day. From August 2020 to January 2021, an average of 140,000 attacks using web shells were recorded each month, and the number is more than doubling every year

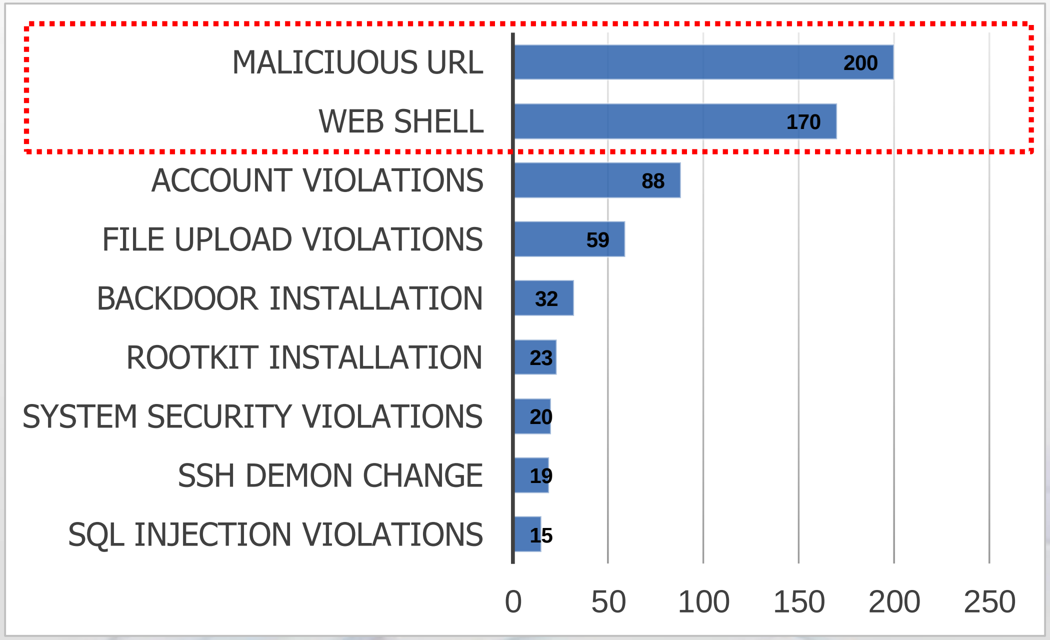
[Source: Web shell attacks continue to rise, Microsoft security Blog]

CYBER ATTACKS



[Source: KISA Security Control Trend]

WEB ATTACKS



[Source: KISA Internet Infringement Response Center / Infringement Trend]

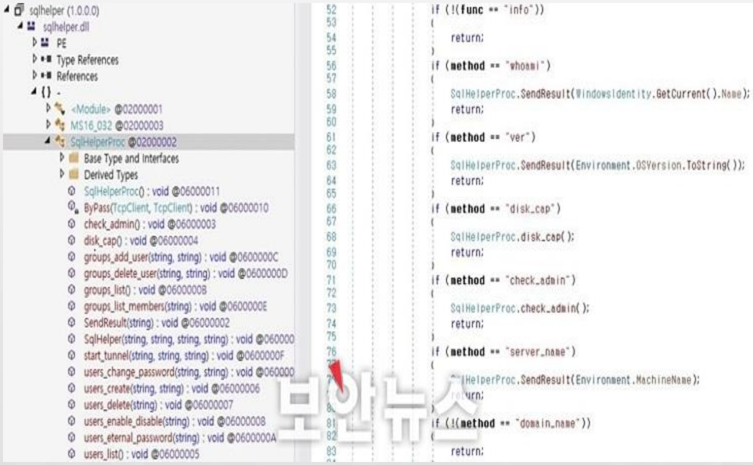
1. Web security overview and necessity

WebShell attack damage case

Trigona ransomware distributed through improperly managed MS-SQL servers

2023-04-12 10:21

Installed not only on Windows servers but also on desktop environments... Detects malware such as Remcos RAT. After installing CLR Shell malware, administrator privileges are acquired and Trigona ransomware is installed and infected. It registers the Trigona binary in the Run key so that it can be run even after rebooting, and then deletes the volume shadow and disables the system restore function, making recovery after ransomware infection impossible.



```
◢ sqlhelper (1.0.0.0)
  ◢ sqlhelper.dll
    ▷ PE
    ▷ Type References
    ▷ References
    ◢ {} -
      ▷ <Module> @02000001
      ▷ MS16_032 @02000003
      ◢ SqlHelperProc @02000002
        ▷ Base Type and Interfaces
        ▷ Derived Types
          SqlHelperProc() : void @06000011
          ByPass(TcpClient, TcpClient) : void @06000010
          check_admin() : void @06000003
          disk_cap() : void @06000004
          groups_add_user(string, string) : void @0600000C
          groups_delete_user(string, string) : void @0600000D
          groups_list() : void @0600000B
          groups_list_members(string) : void @0600000E
          SendResult(string) : void @06000002
          SqlHelper(string, string, string, string) : void @060000
          start_tunnel(string, string, string) : void @0600000F
          users_change_password(string, string) : void @060000
          users_create(string, string) : void @06000006
          users_delete(string) : void @06000007
          users_enable_disable(string) : void @06000008
          users_eternal_password(string) : void @0600000A
          users_list() : void @06000005
```

```
if (!(func == "info"))
{
    return;
}
if (method == "whoami")
{
    SqlHelperProc.SendResult(WindowsIdentity.GetCurrent().Name);
    return;
}
if (method == "ver")
{
    SqlHelperProc.SendResult(Environment.OSVersion.ToString());
    return;
}
if (method == "disk_cap")
{
    SqlHelperProc.disk_cap();
    return;
}
if (method == "check_admin")
{
    SqlHelperProc.check_admin();
    return;
}
if (method == "server_name")
{
    SqlHelperProc.SendResult(Environment.MachineName);
    return;
}
if (!(method == "domain_name"))
{
    return;
```

▲CLR Shell malware used in attack [Data = AhnLab ASEC Analysis Team]

Chinese hacker organization Xiaoqing discloses personal information database of three hacked academic institutions to the dark web

2023-01-29 14:27

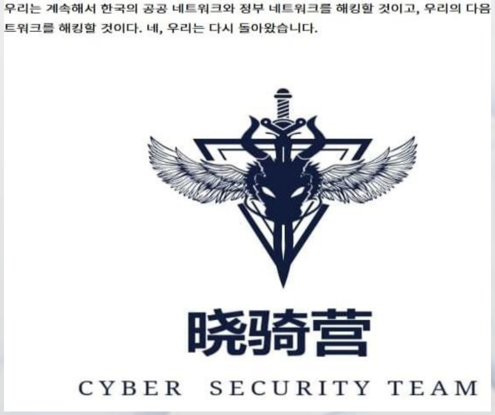
Personal information such as mobile phone number and address that appears to be member information is disclosed to the internal databases of three organizations, the Korean Archaeological Society, the Korean Educational Principles Society, and the Korean Parents' Association, on the dark web forum.

Including...there is a possibility of past leaked information.

SQL commands were sent through the web and web administrator account information stored in the database was stolen. (Insert webshell)

Xiaoqing stole or deleted internal company information through hacking.

They also altered websites into their own web pages or created them without permission.



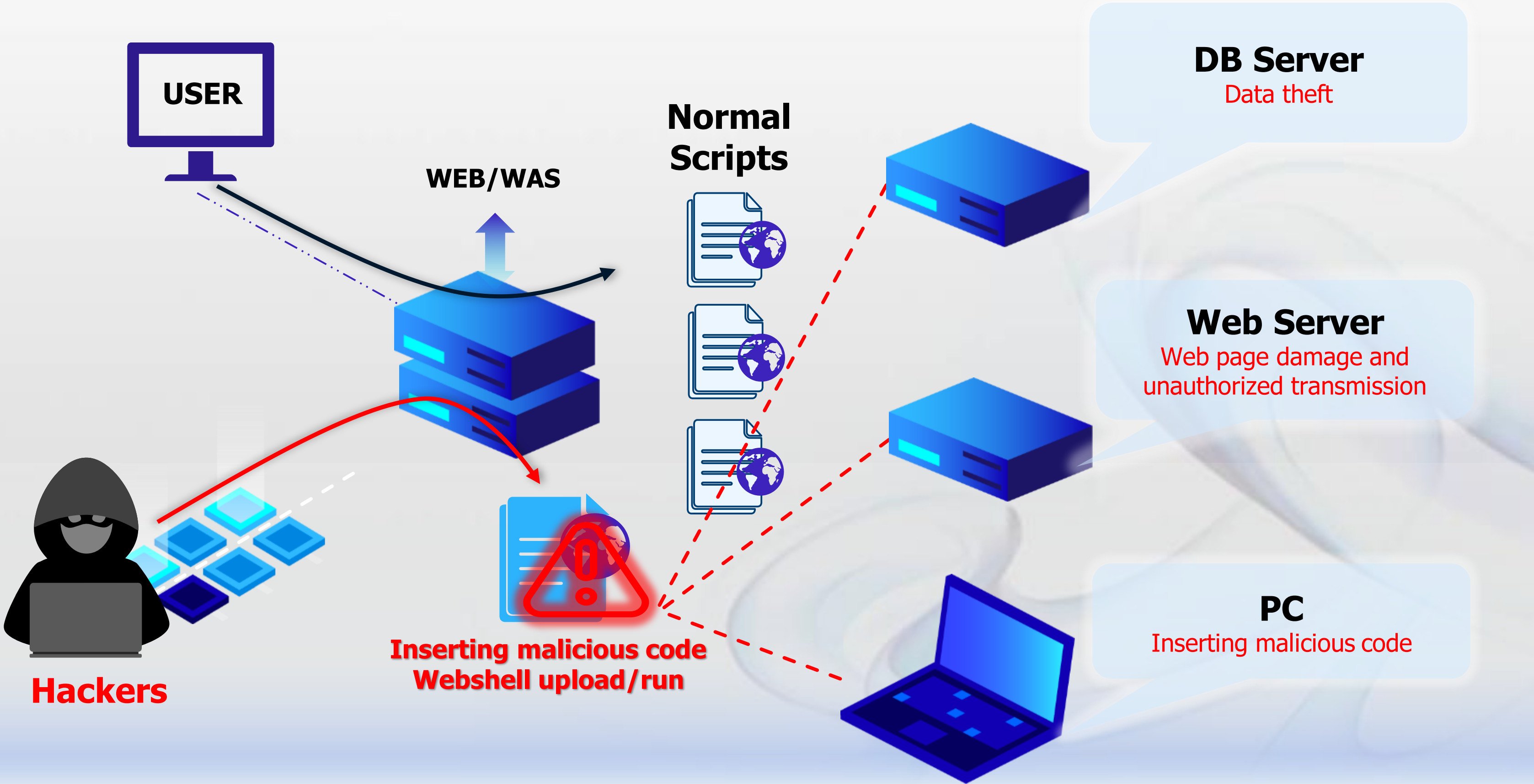
우리는 계속해서 한국의 공공 네트워크와 정부 네트워크를 해킹할 것이고, 우리의 다음
트워크를 해킹할 것이다. 네, 우리는 다시 돌아왔습니다.

◀ Type of web page uploaded to the website hacked by Xiaoqing/ Photo provided by Korea Internet & Security Agency

1. Web security overview and necessity

What is web-based “Malware” or “WebShell”?

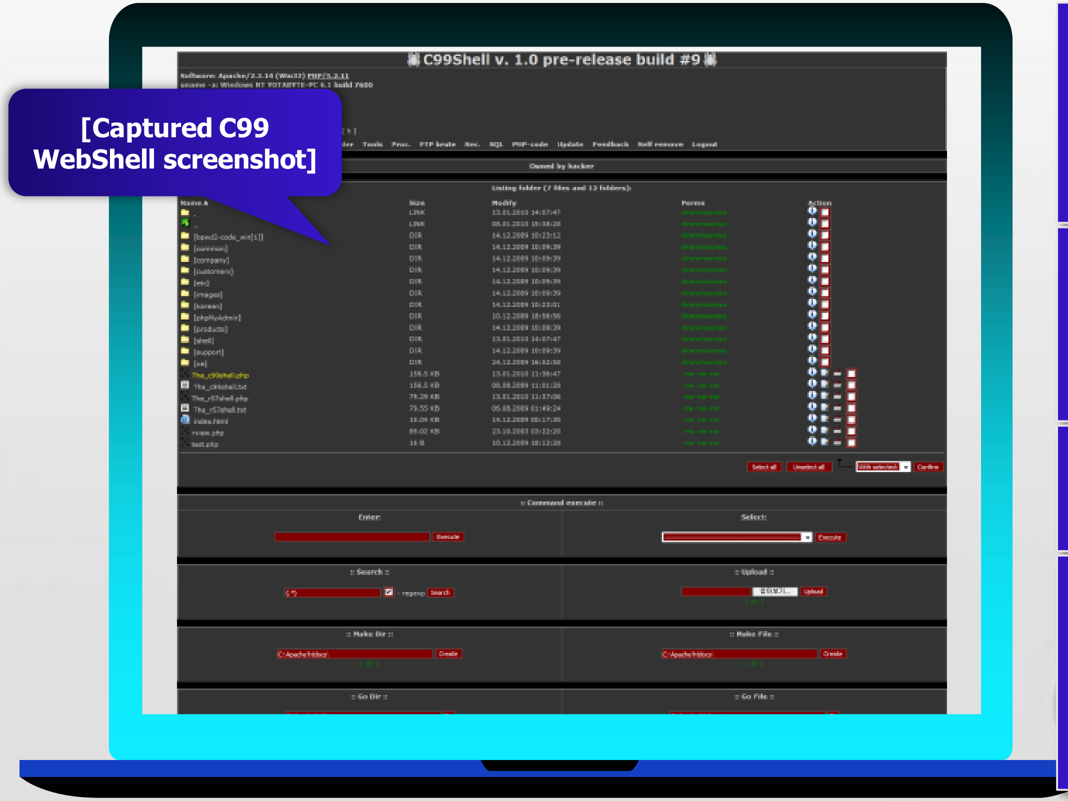
- It is an instruction program that is inserted by exploiting vulnerabilities in a web server, and when executed as a server-side script (ASP, JSP, PHP, CGI, PYTHON, etc.), it can take control of the server equivalent to root privileges.
- Web service ports for web services (http (80, 8080), https (443)) act as backdoors and are subject to severe hacking attacks, such as stealing confidential data, corrupting web pages and passing access to unauthorized pages, and spreading malware.



1. Web security overview and necessity

Web-based malware/ "Webshell"

- Webshell avoids security systems and allows easy access to existing systems without separate authentication.
- Webshells are fatally dangerous because they are difficult to recognize unless a hacking incident occurs.



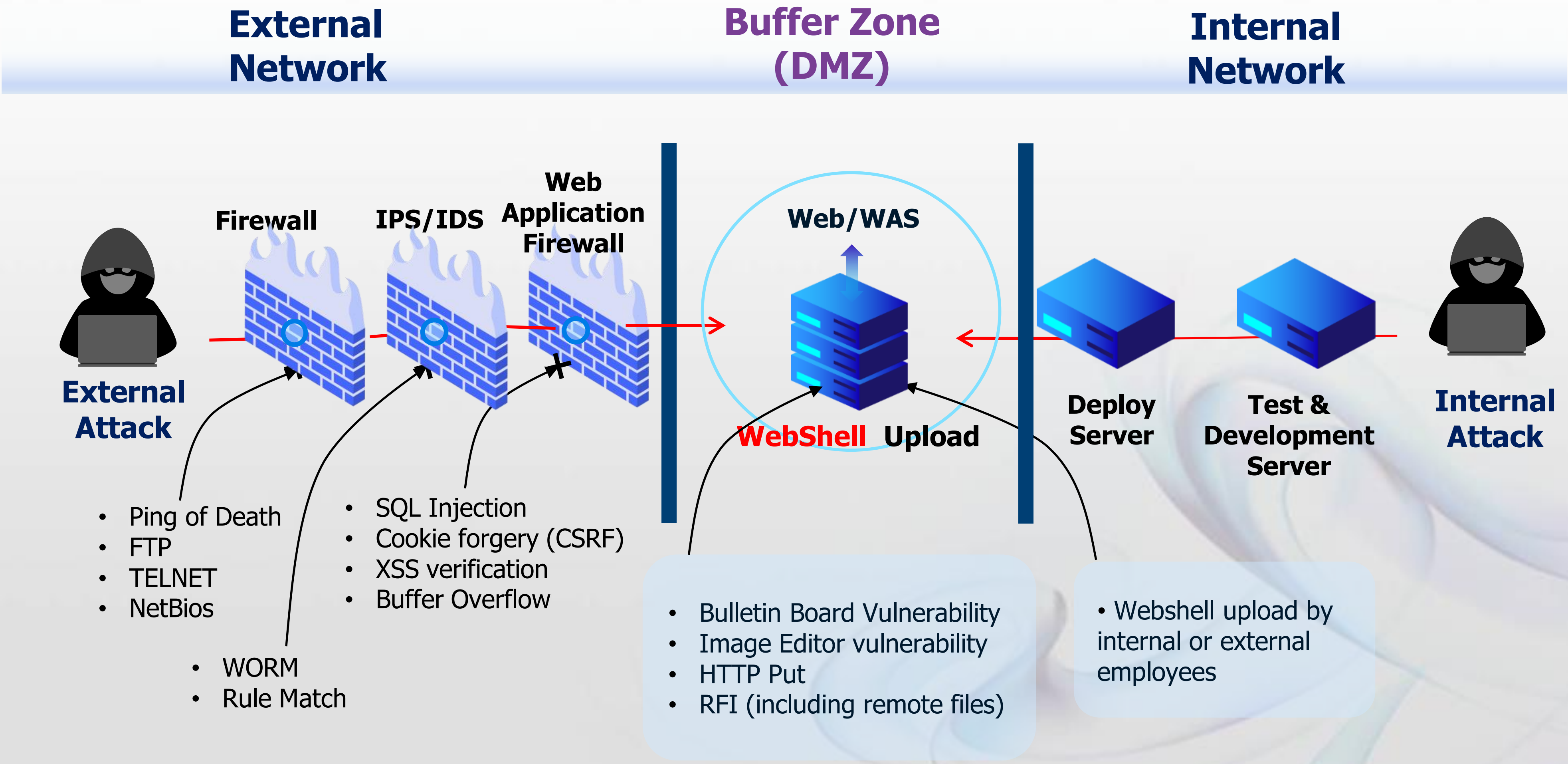
```
C99Shell v. 1.0 pre-release build #9
Software: Apache/2.2.14 (Win32) PHP/5.2.11
uname -a: Windows NT YOTABYTE-PC 6.1 build 7600
[ h ]
...der  Tools  Proc.  FTP brute  Sec.  SQL  PHP-code  Update  Feedback  Self remove  Logout
Owned by hacker
Listing folder (7 files and 12 folders):
Name ▲                    Size      Modify                 Perms        Action
.                         LINK      13.01.2010 14:07:47    drwxrwxrwx
..                        LINK      08.01.2010 15:38:20    drwxrwxrwx
[bpwd2-code_win[1]]       DIR       14.12.2009 10:23:12    drwxrwxrwx
[common]                  DIR       14.12.2009 10:09:39    drwxrwxrwx
[company]                 DIR       14.12.2009 10:09:39    drwxrwxrwx
[customers]               DIR       14.12.2009 10:09:39    drwxrwxrwx
[etc]                     DIR       14.12.2009 10:09:39    drwxrwxrwx
[images]                  DIR       14.12.2009 10:09:39    drwxrwxrwx
[korean]                  DIR       14.12.2009 10:23:01    drwxrwxrwx
[phpMyAdmin]              DIR       10.12.2009 18:56:56    drwxrwxrwx
[products]                DIR       14.12.2009 10:09:39    drwxrwxrwx
[shell]                   DIR       13.01.2010 14:07:47    drwxrwxrwx
[support]                 DIR       14.12.2009 10:09:39    drwxrwxrwx
[xe]                      DIR       24.12.2009 16:12:38    drwxrwxrwx
The_c99shell.php          156.5 KB  13.01.2010 11:36:47    -rw-rw-rw-
The_c99shell.txt          156.5 KB  08.08.2009 11:01:20    -rw-rw-rw-
The_r57shell.php          79.29 KB  13.01.2010 11:37:06    -rw-rw-rw-
The_r57shell.txt          79.55 KB  06.08.2009 01:49:24    -rw-rw-rw-
index.html                10.04 KB  14.12.2009 00:17:30    -rw-rw-rw-
rview.php                 89.02 KB  23.10.2003 03:22:20    -rw-rw-rw-
test.php                  16 B      10.12.2009 18:12:20    -rw-rw-rw-
                                  [Select all] [Unselect all] [With selected: ▾] [Confirm]
:: Command execute ::
Enter:  [Execute]                              Select:  [▾] [Execute]
:: Search ::                                   :: Upload ::
[*] ☑ - regexp [Search]                        [Upload]
:: Make Dir ::                                 :: Make File ::
C:\Apache\htdocs\ [Create]                     C:\Apache\htdocs\ [Create]
:: Go Dir ::                                   :: Go File ::
```

[Captured C99 WebShell screenshot]

System Command	- View system information - System Shutdown - Stop/remove specific programs (Example: Anti-Virus program)
Network	- port scanner - TELNET, SSH, FTP - Access (internal network access possible)
Database	- Data leakage, alteration, deletion
System File	- Hacking tool upload (keylog, backdoor) - Modifying files (inserting malicious code) - Delete system files - View all system directories

1. Web security overview and necessity

Intrusion route of malicious code (WebShell)



- Ping of Death
- FTP
- TELNET
- NetBios

- WORM
- Rule Match

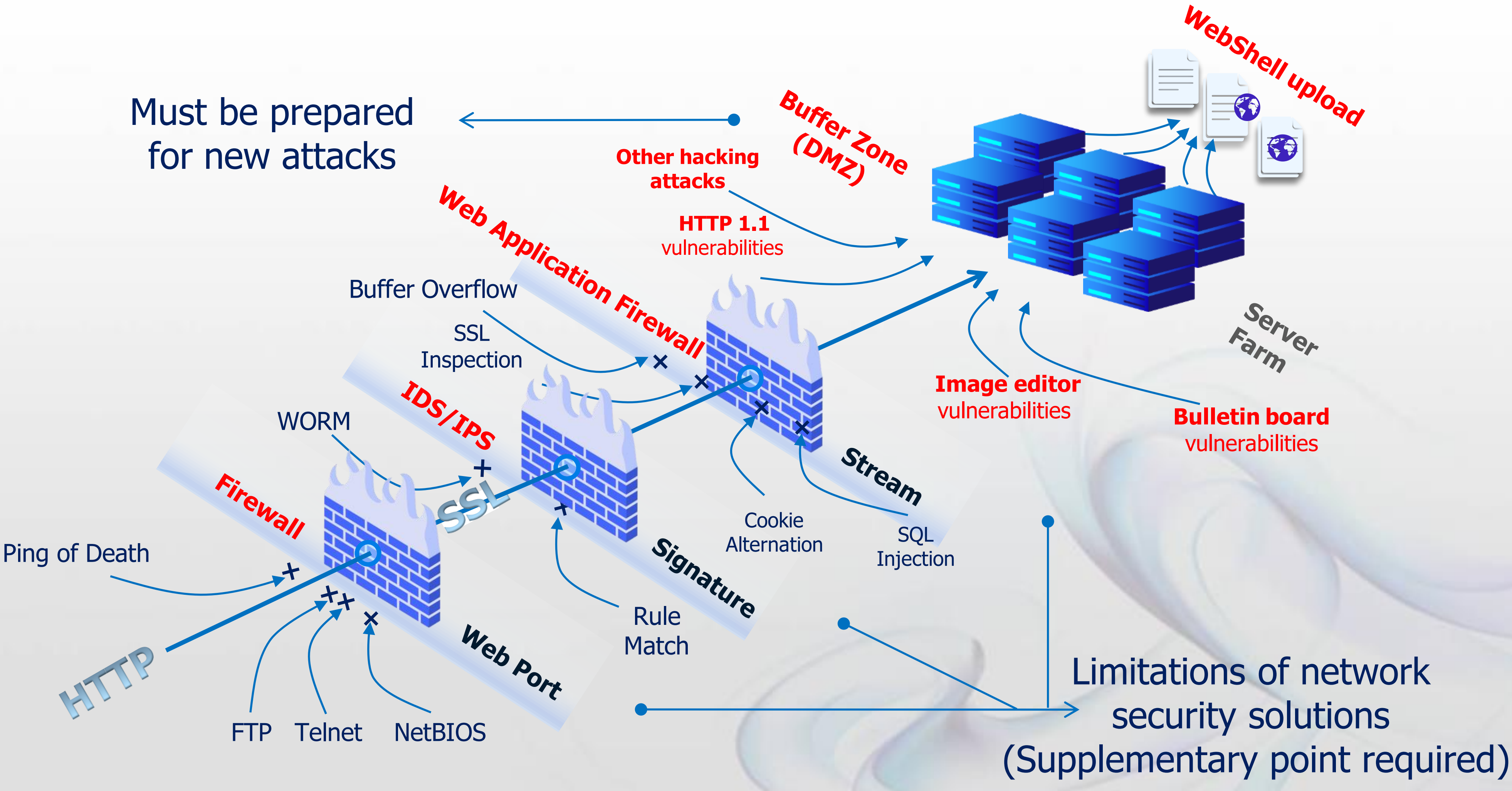
- SQL Injection
- Cookie forgery (CSRF)
- XSS verification
- Buffer Overflow

- Bulletin Board Vulnerability
- Image Editor vulnerability
- HTTP Put
- RFI (including remote files)

- Webshell upload by internal or external employees

1. Web security overview and necessity

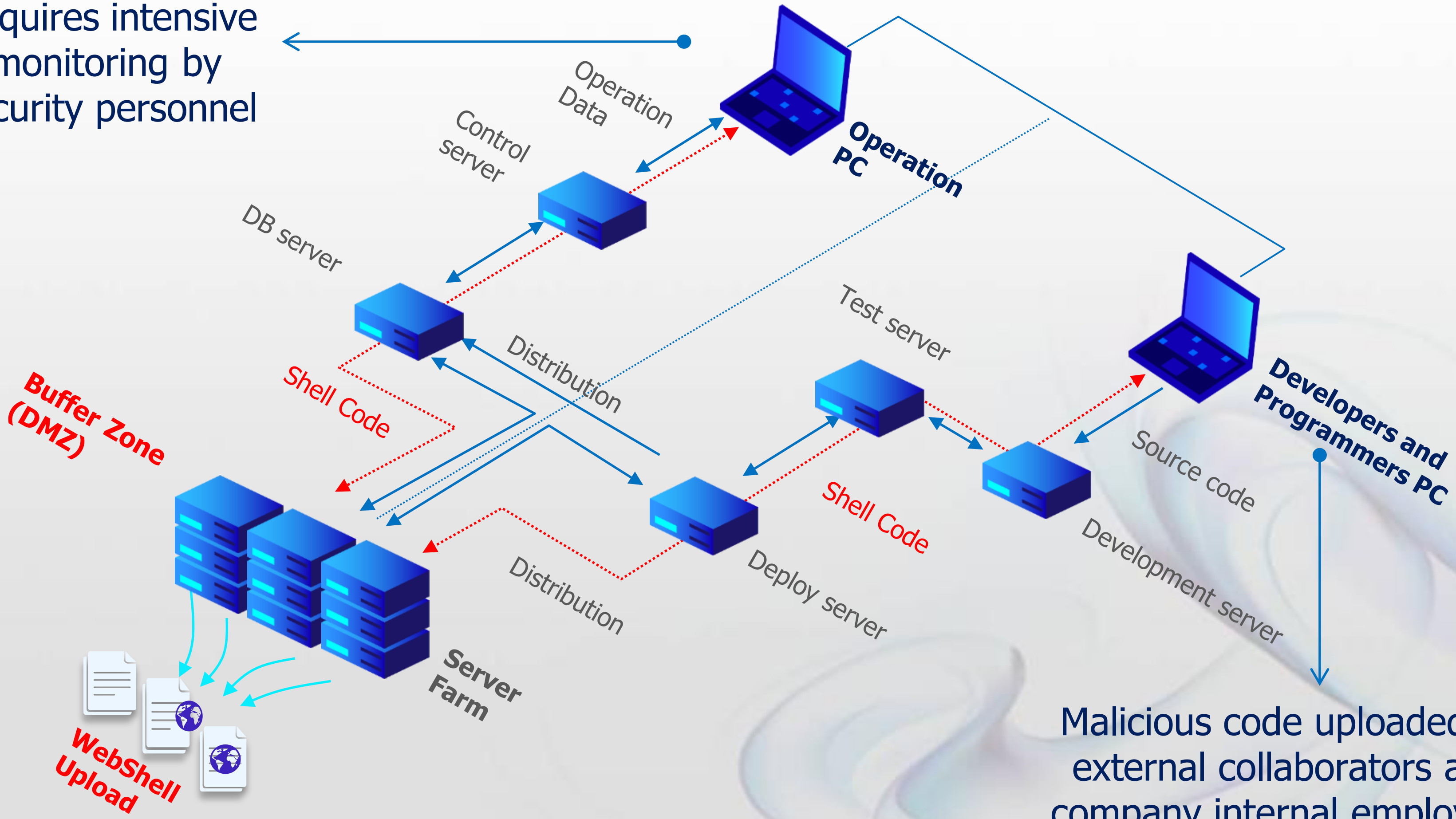
Intrusion From External Network



1. Web security overview and necessity

Intrusion From Internal Network

Requires intensive monitoring by security personnel

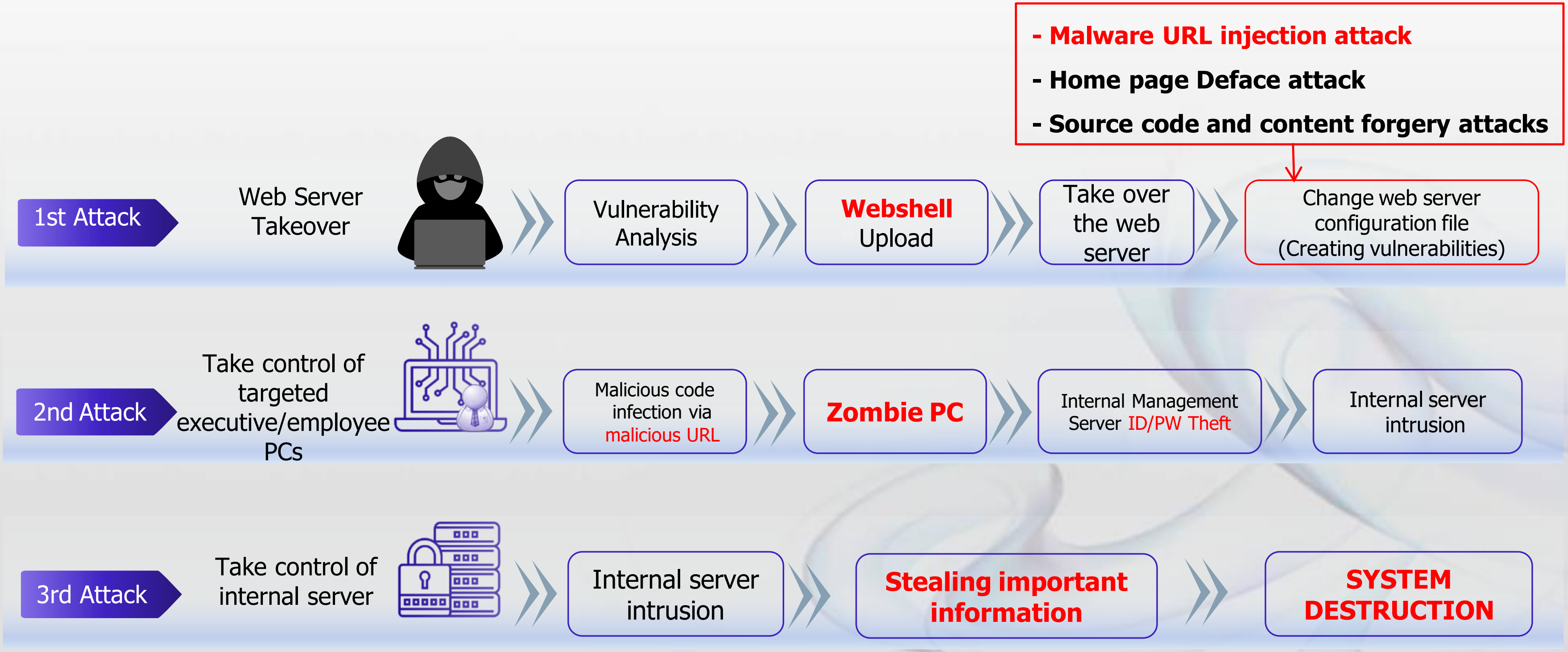


Malicious code uploaded by external collaborators and company internal employees with impure intentions

1. Web security overview and necessity

Web Hacking Process

Recently, web hacking is a complex and continuous attempt (APT attack) based on web shells, and is carried out step by step with an accurate attack target.



- **Malware URL injection attack**
- **Home page Deface attack**
- **Source code and content forgery attacks**

1st Attack: Web Server Takeover » Vulnerability Analysis » **Webshell** Upload » Take over the web server » Change web server configuration file (Creating vulnerabilities)

2nd Attack: Take control of targeted executive/employee PCs » Malicious code infection via malicious URL » **Zombie PC** » Internal Management Server ID/PW Theft » Internal server intrusion

3rd Attack: Take control of internal server » Internal server intrusion » **Stealing important information** » **SYSTEM DESTRUCTION**

1. Web security overview and necessity

Web Attack Type

Potential risk factors caused by internal and external partner employees

Network security solution Attacks targeting vulnerabilities

- Network security equipment vulnerabilities (analyzed by packet)
- Anti-virus compiled binary-based malware attack

Web Hacking

Bulletin board upload attack Upload attack using source code vulnerabilities

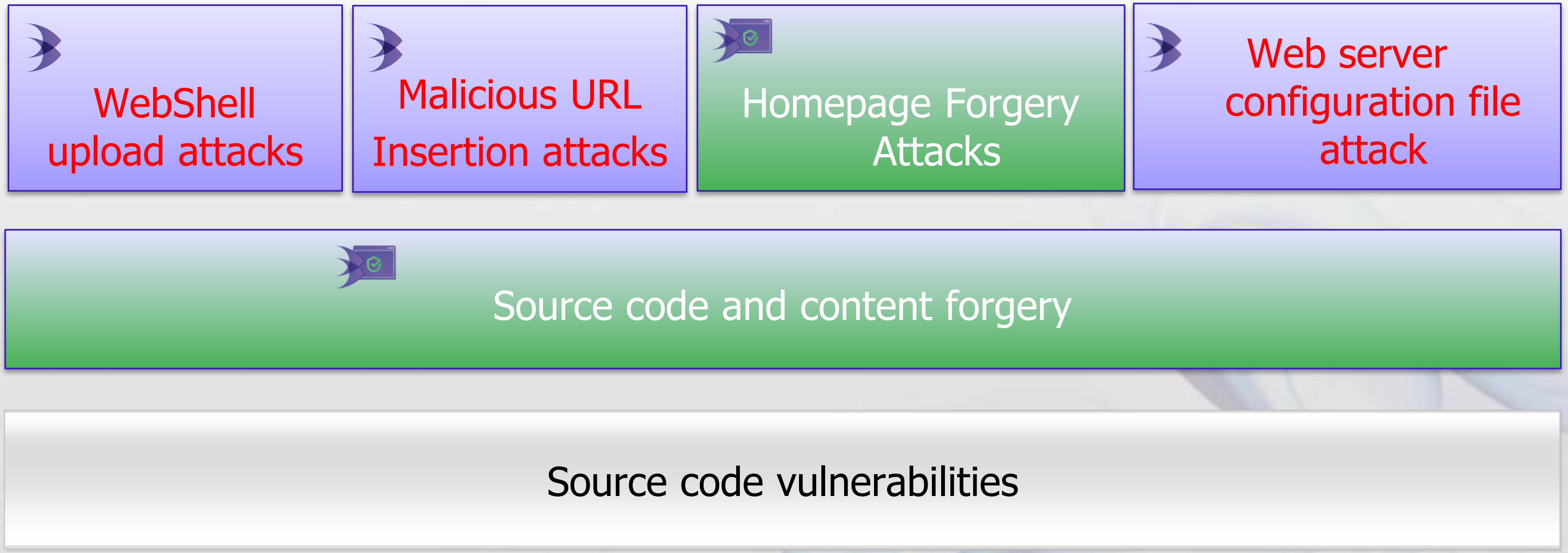
- Extension tampering vulnerability
- Attack disguised as an image file

Web server/WAS OS Zero Day Vulnerability Attack

1. Web security overview and necessity

Types of Web Attacks

Major web-based attacks take advantage of web source code vulnerabilities and lead to source code and data modification, which takes the form of attacks such as web shells, malicious URLs, homepage forgery, and web server configuration file modification.



WebShell upload attacks

Malicious URL Insertion attacks

Homepage Forgery Attacks

Web server configuration file attack

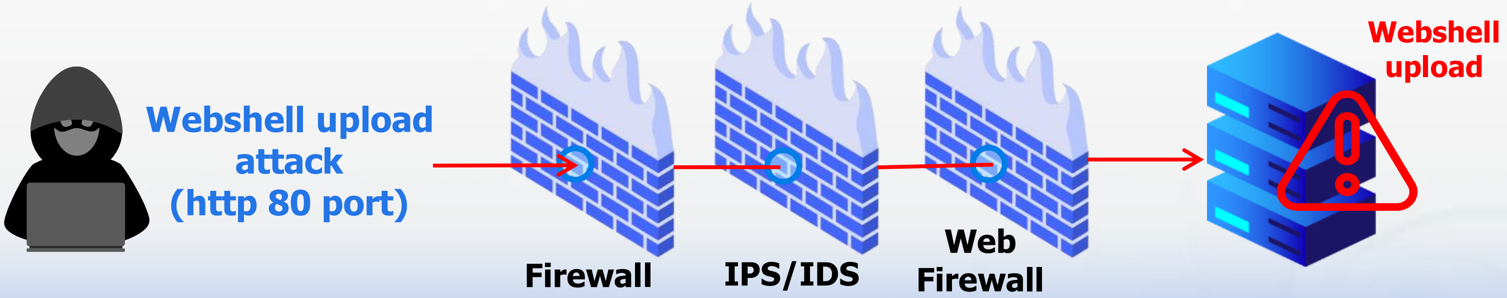
Source code and content forgery

Source code vulnerabilities

Types of Web Attacks

Webshell upload attack

Once uploaded and executed on a web server, server control equivalent to root authority is possible.



System Commands	Network Commands	System File Access	Database Access	User PC
• View system information • System shutdown • Stop/delete specific program (Anti-virus software, etc.)	• Port scanner • TELNET, SSH, FTP access (access internal network)	• Hacking tool upload (keylog, backdoor) • File modification (malware insertion) • Delete system files • View system directory	• Data Breach • Changing data • Deleting data	• Malware Infection • Data breach • Administrator's main system access information leaked • Trigger a DDoS attack

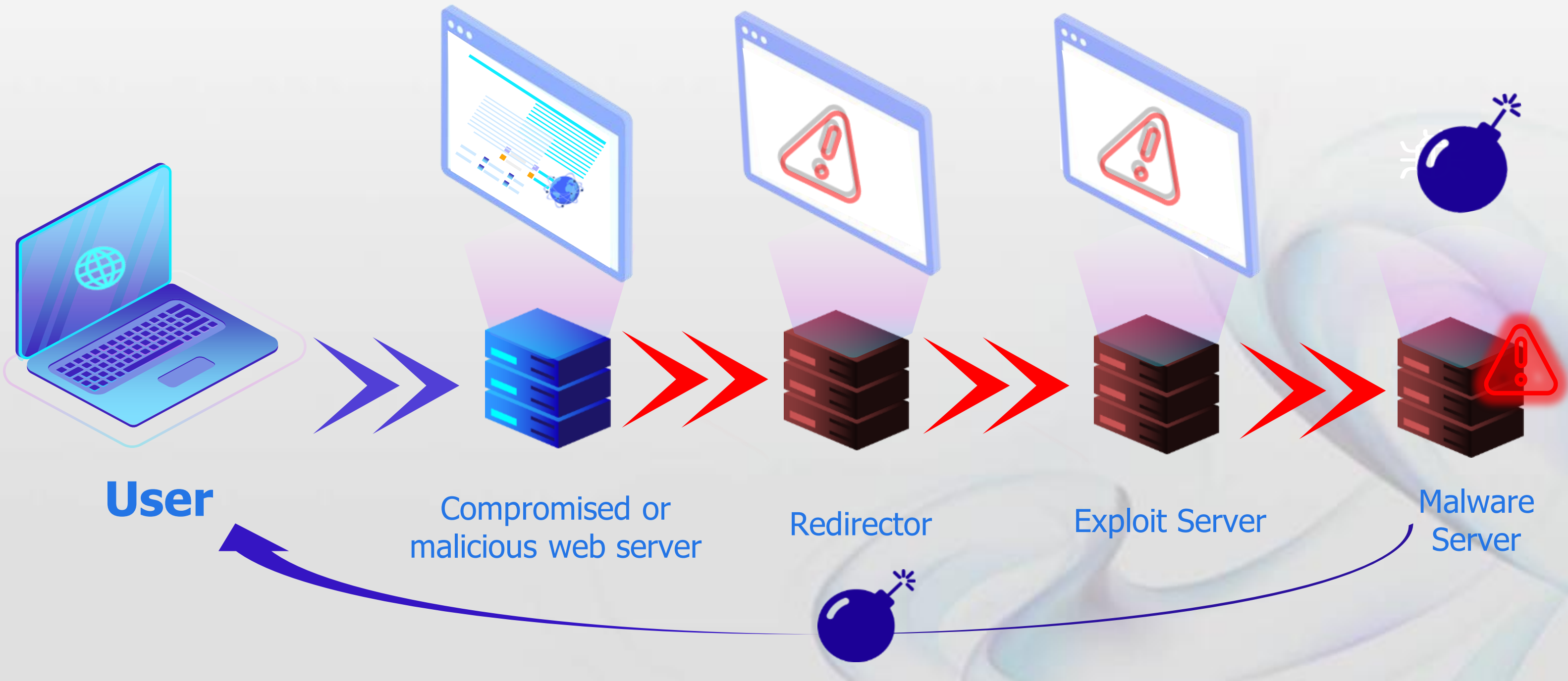
1. Web security overview and necessity

WEBSERVER SAFEGUARD

Types of Web Attacks

Malicious URL injection attack

Malicious URLs are URLs or IP addresses that use web servers as a transit point for malicious code to distribute viruses, ransomware, etc. to PCs in large quantities, and can cause serious damage such as file encryption, personal information leaks, and DDoS attacks.



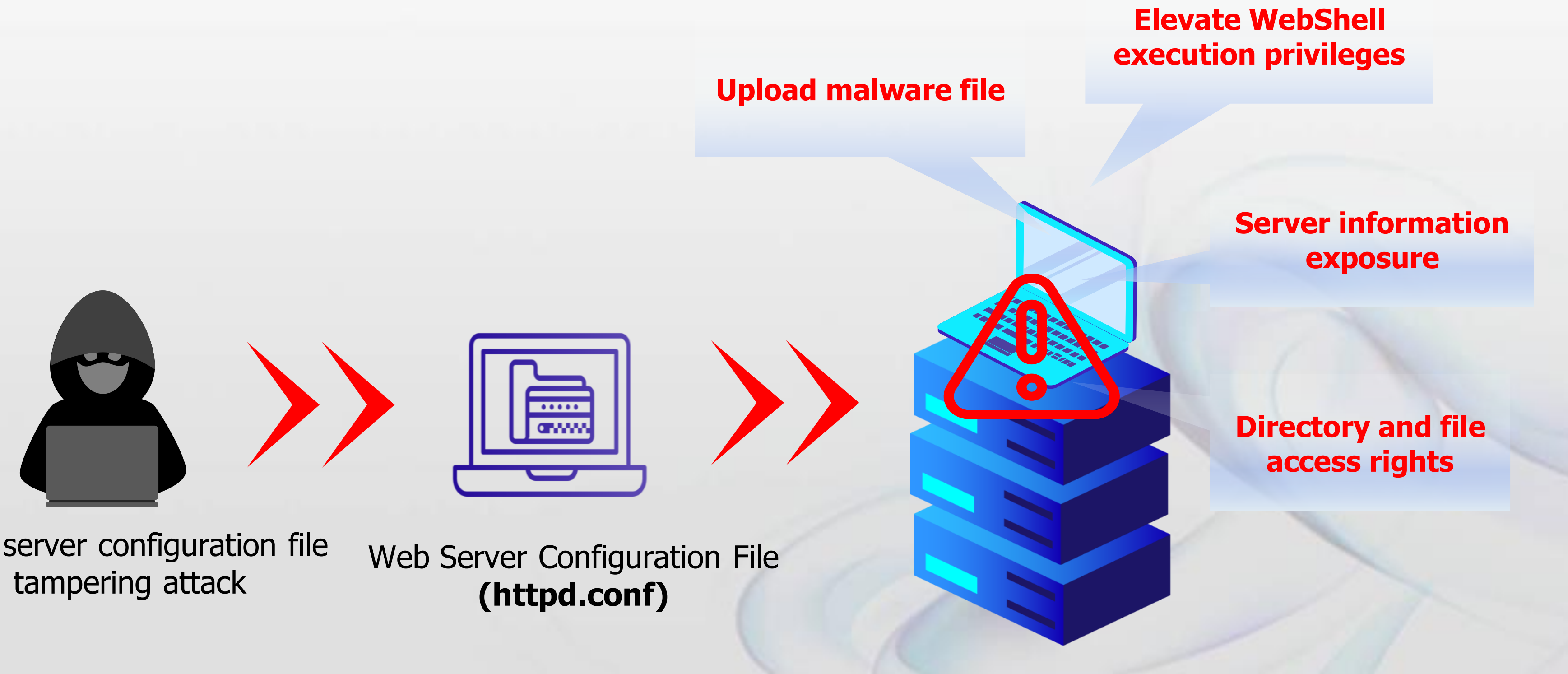
Source : MS Security intelligence report

1. Web security overview and necessity

Types of Web Attacks

Web server configuration file tampering attack

Hackers modify web server configuration files to create new vulnerabilities and use them as a secondary attack path.


Upload malware file
Elevate WebShell execution privileges
Server information exposure
Directory and file access rights
Web server configuration file tampering attack
Web Server Configuration File
(httpd.conf)

CONTENT

1. Web security overview and necessity

2. Introduction to WSS (overview and structure)

3. WSS main features

4. WSS main function

2. Introduction to WSS (overview and structure)

WSS (Web Server Safeguard)?

WSS is a webshell-specific security solution that ensures safe operation of web servers by real-time monitoring of 'webshell', a malicious program used for web server hacking.

WSS
INFORMATION SECURITY WITH UNINTERRUPTED SERVICE
Webserver Security Solution
On-Premise
umv
WSS CLOUD
Webserver Security Solution
CLOUD

Webshell detection and action

Malicious URL detection and action

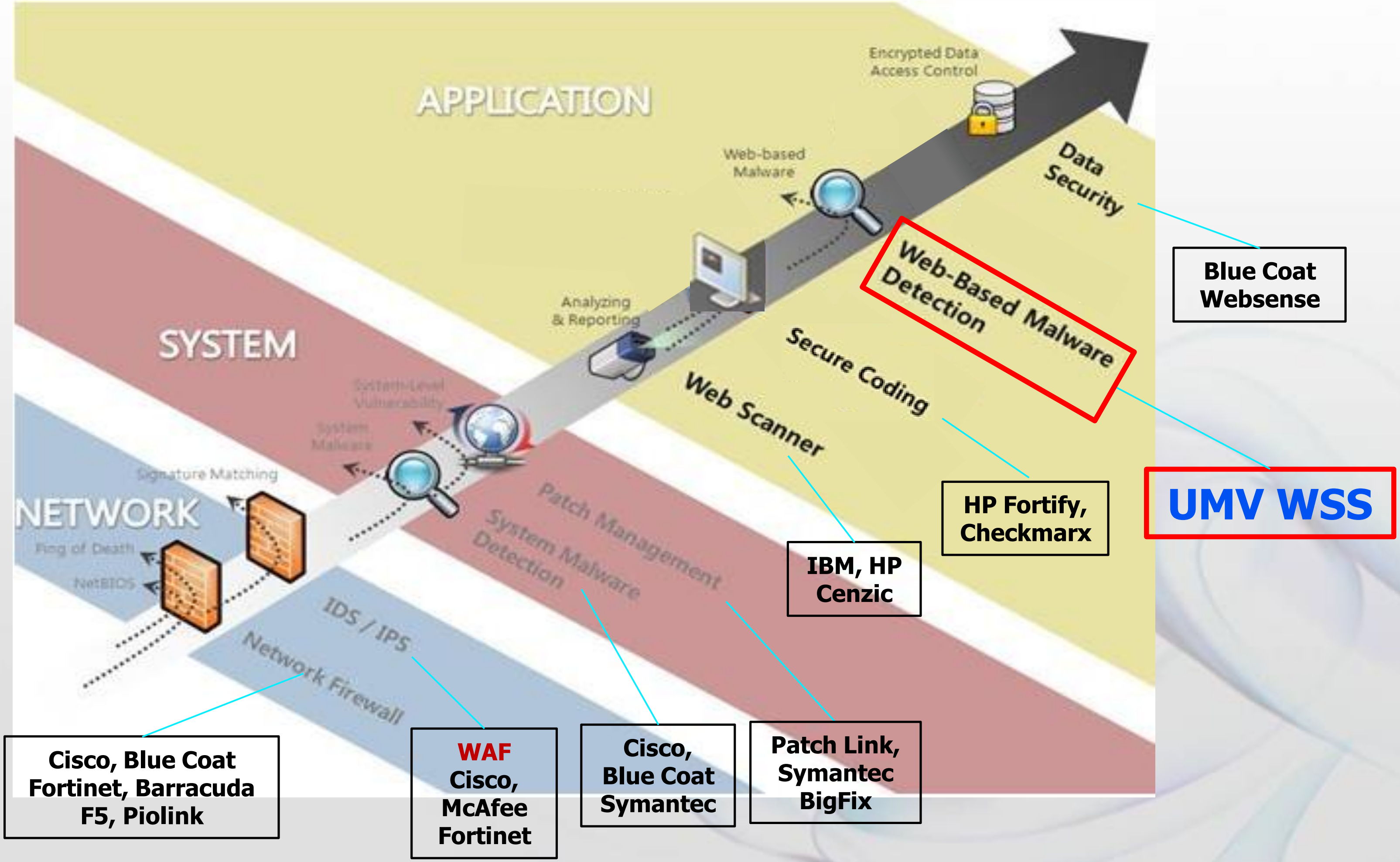
Prevent changes to web server configuration files

Cloud computing VM, Docker support

2. Introduction to WSS (overview and structure)

WSS Positioning

Web Security 3 Tier and Solutions



Blue Coat
Websense

UMV WSS

HP Fortify,
Checkmarx

IBM, HP
Cenzic

Cisco, Blue Coat
Fortinet, Barracuda
F5, Piolink

WAF
Cisco,
McAfee
Fortinet

Cisco,
Blue Coat
Symantec

Patch Link,
Symantec
BigFix

2. Introduction to WSS (overview and structure)

WSS Positioning

WEB Application Security

- The core of Web Security is Web Application Security.
- Application Security should took care of very carefully from early stages of Development to maintenance after finishing to build.

▷ **Web Scanner**

The program that analyze potential vulnerability or vulnerabilities on design via communication outside of web application.

▷ **Secure Coding**

Writing code for considering security from design phase to minimize the vulnerability that may result from various cause such as lack of knowledge or mistakes of developers in development process.

▷ **Web-Based Malware Detection**

In an existing working web application, the web shell is detected and removed in real time as a source code, notified the administrator, and the inserted web shell is almost difficult to detect. Hackers use this web shell for multiple purposes to hack

▷ **Data Security**

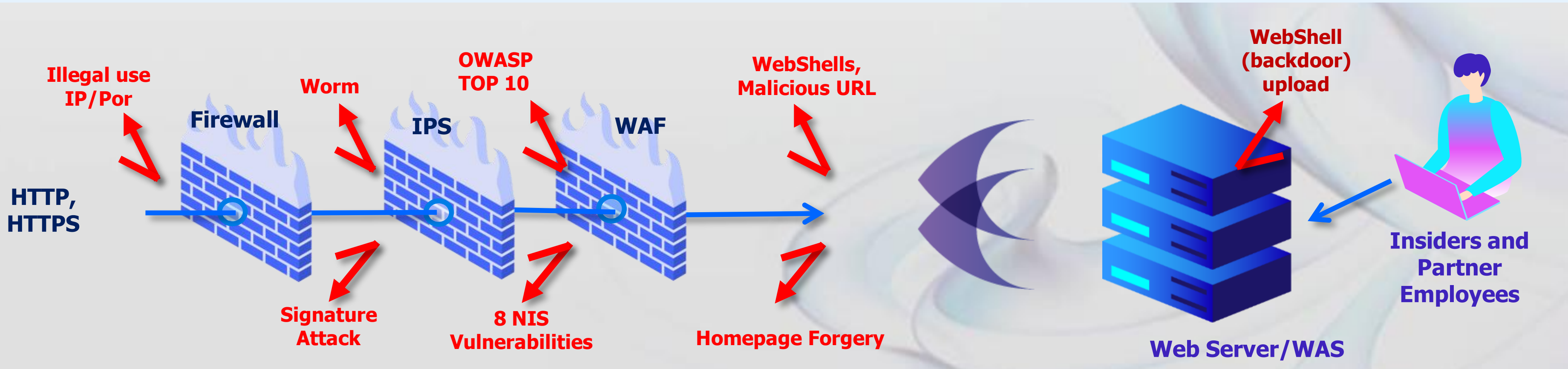
In general, build database and stores data in web application environment, data security manage these data safely.

Why WSS (Web Server Safeguard)?

WSS defends against various web attacks by hackers through web application vulnerabilities.

* Complementary relationship with WAF (Web Application Firewall), a network security appliance

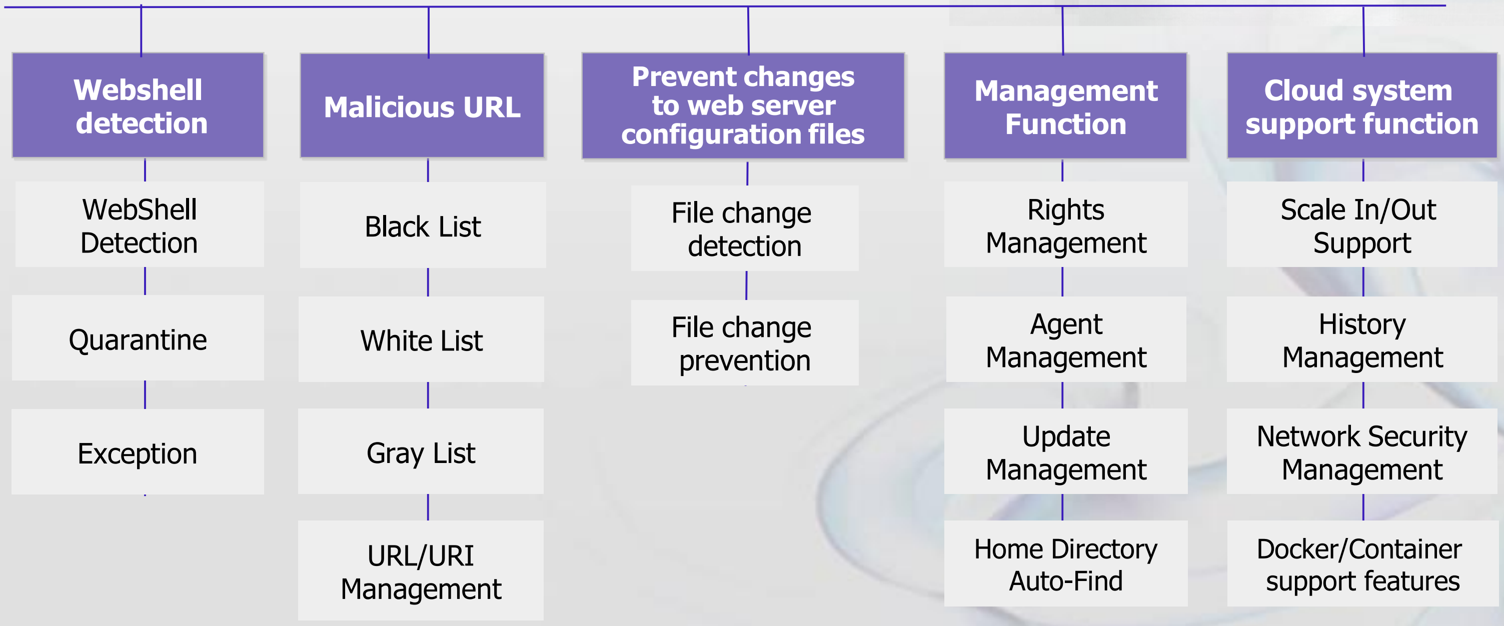
- There are limitations in network defense due to the diversification of intrusion methods (emerging need to detect/quarantine web server malware within the system)
- Increase in information security incidents caused not only by external hacking but also by users within the organization
- Unable to detect web server malware that penetrated before installing a web application firewall
- Overload for full inspections
- Possible penetration through network bypass vulnerability
- Risks of encryption/encoding traffic and security policy exception handling



2. Introduction to WSS (overview and structure)

Overview and Key Features

Product Name	WSS (Web Server Safeguard)
Latest Version	v2.7
Release Date	May 2010
Manufacturer	UMV Inc.



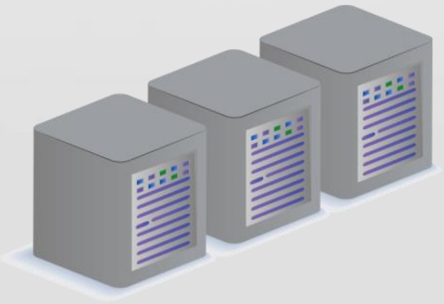
- **Webshell detection**
  - WebShell Detection
  - Quarantine
  - Exception
- **Malicious URL**
  - Black List
  - White List
  - Gray List
  - URL/URI Management
- **Prevent changes to web server configuration files**
  - File change detection
  - File change prevention
- **Management Function**
  - Rights Management
  - Agent Management
  - Update Management
  - Home Directory Auto-Find
- **Cloud system support function**
  - Scale In/Out Support
  - History Management
  - Network Security Management
  - Docker/Container support features

2. Introduction to WSS (overview and structure)

Configuring the WSS solution

Consists of management server, agent, and manager program (PC)

WSS Management server	WSS Agent	Manager program (PC)
• Server SW installed on VM or HW Works by connecting to WSS Agent • Save detection history and detection information • Remote management control • In addition to webshell pattern updates and agent deployment	• Program installed on web server/WAS • Webshell detection and malicious distribution URL detection • Webshell detection and filtering progress server transfer, etc. • JDK 1.5 supported Unix, Linux, NT O/S support	• Installation on administrator-operated PC (Connect to WSS management server) • Run webshell detection • Monitoring, remote action, environmental settings • Administrator authority management, statistics & reporting, etc.



2. Introduction to WSS (overview and structure)

WSS detection method

Collects malware to improve detection performance.

✓ **Analysis of detection history of over 30,000 applied agents**

✓ **Operate personnel specialized in malicious code collection and analysis**

Pattern detection

- Detection by comparing the existing webshell pattern with the pattern of the detected file.
- Generate webshell patterns with signatures / detect known webshells.

Hash value detection

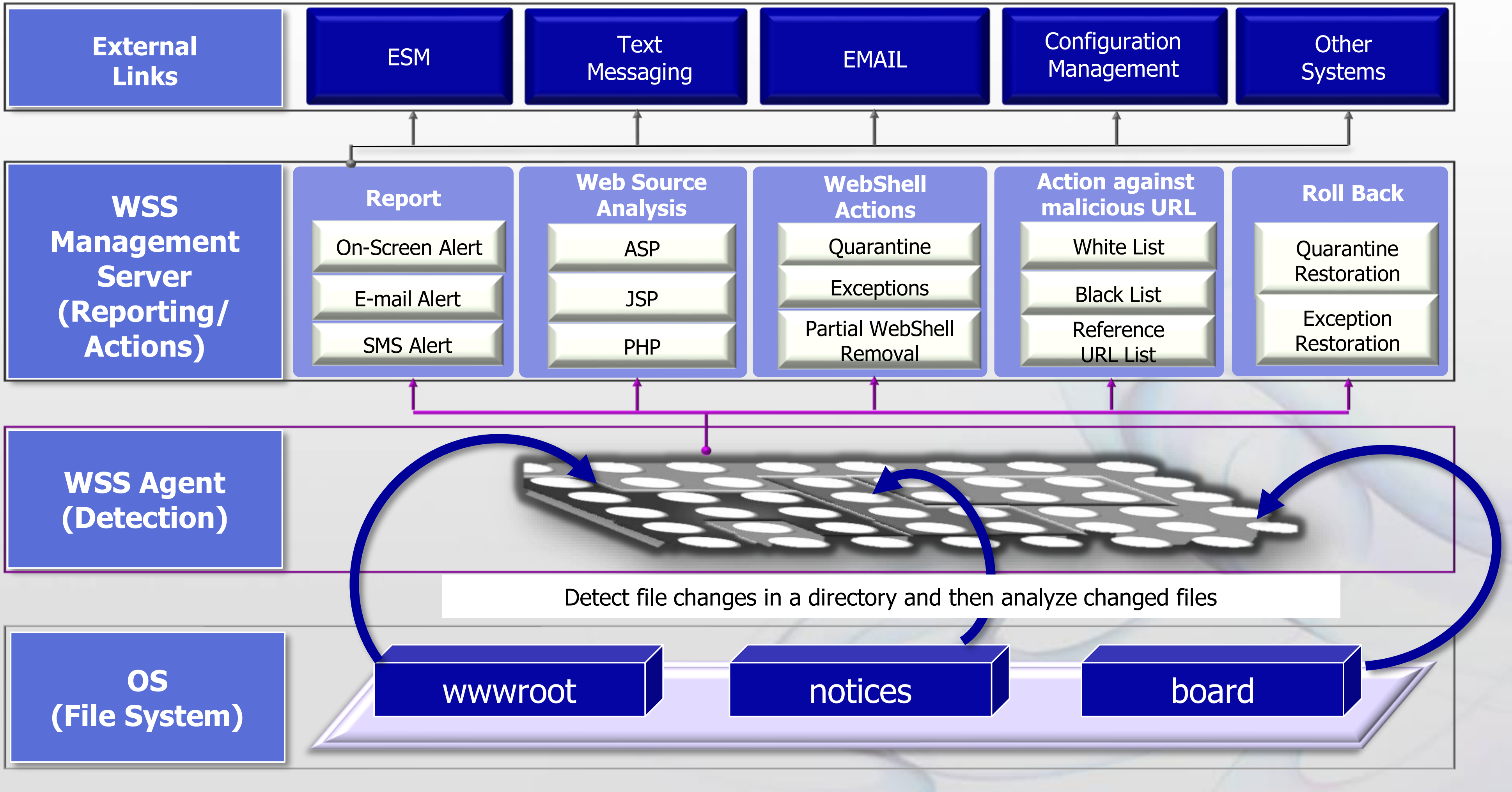
- If the pattern continues to increase, the system speed deteriorates. For efficient performance, WSS detects by periodically updating the hash value provided by www.virustotal.com a malicious code sharing portal.

Algorithm detection

- Detects obfuscated or encoded web shells such as JAVA Script through internal code.

Structure and operating principle

Detects tampering and generated malicious code through file system monitoring.



External Links

ESM

Text Messaging

EMAIL

Configuration Management

Other Systems

WSS Management Server (Reporting/ Actions)

Report
- On-Screen Alert
- E-mail Alert
- SMS Alert

Web Source Analysis
- ASP
- JSP
- PHP

WebShell Actions
- Quarantine
- Exceptions
- Partial WebShell Removal

Action against malicious URL
- White List
- Black List
- Reference URL List

Roll Back
- Quarantine Restoration
- Exception Restoration

WSS Agent (Detection)

Detect file changes in a directory and then analyze changed files

OS (File System)

wwwroot

notices

board

CONTENT

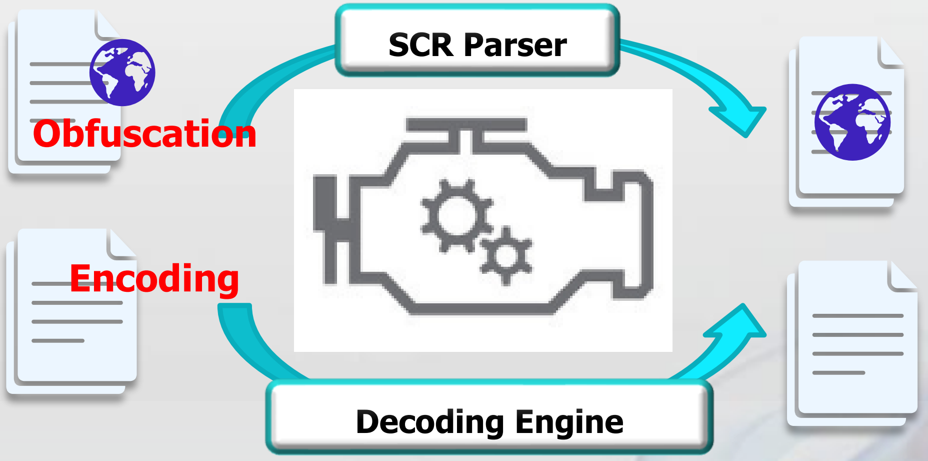
1. Web Security Overview
2. Introduction to WSS (overview and structure)
3. **WSS main features**
4. WSS main function

3. WSS main features

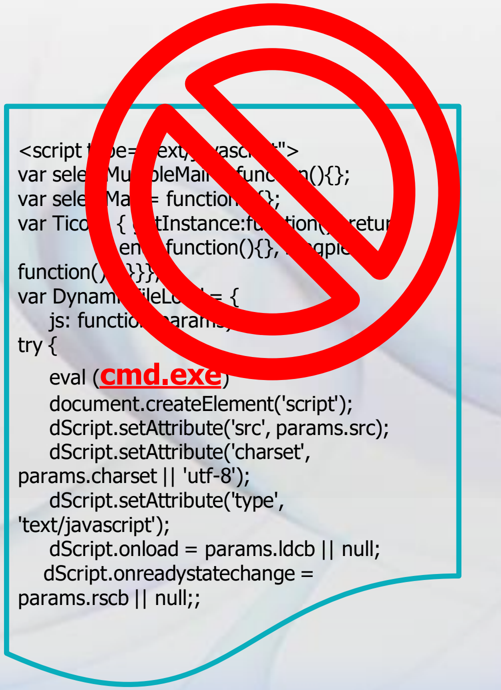
Excellent detection performance

- WSS supports detection of unknown malware through an analysis engine dedicated to obfuscation (SCR Parser).
- Malware collection to improve detection performance
  - Analysis of agent detection history applied to over 30,000 units
  - Operation of experts in malicious code collection and analysis
- Supports sophisticated pattern application and exception handling to minimize false positives
- Supports pattern customization considering the environment for each web server/WAS

Script Files



SCR Parser (Source Code Recombinant Parser)
Dedicated engine for analyzing and detecting obfuscated source code

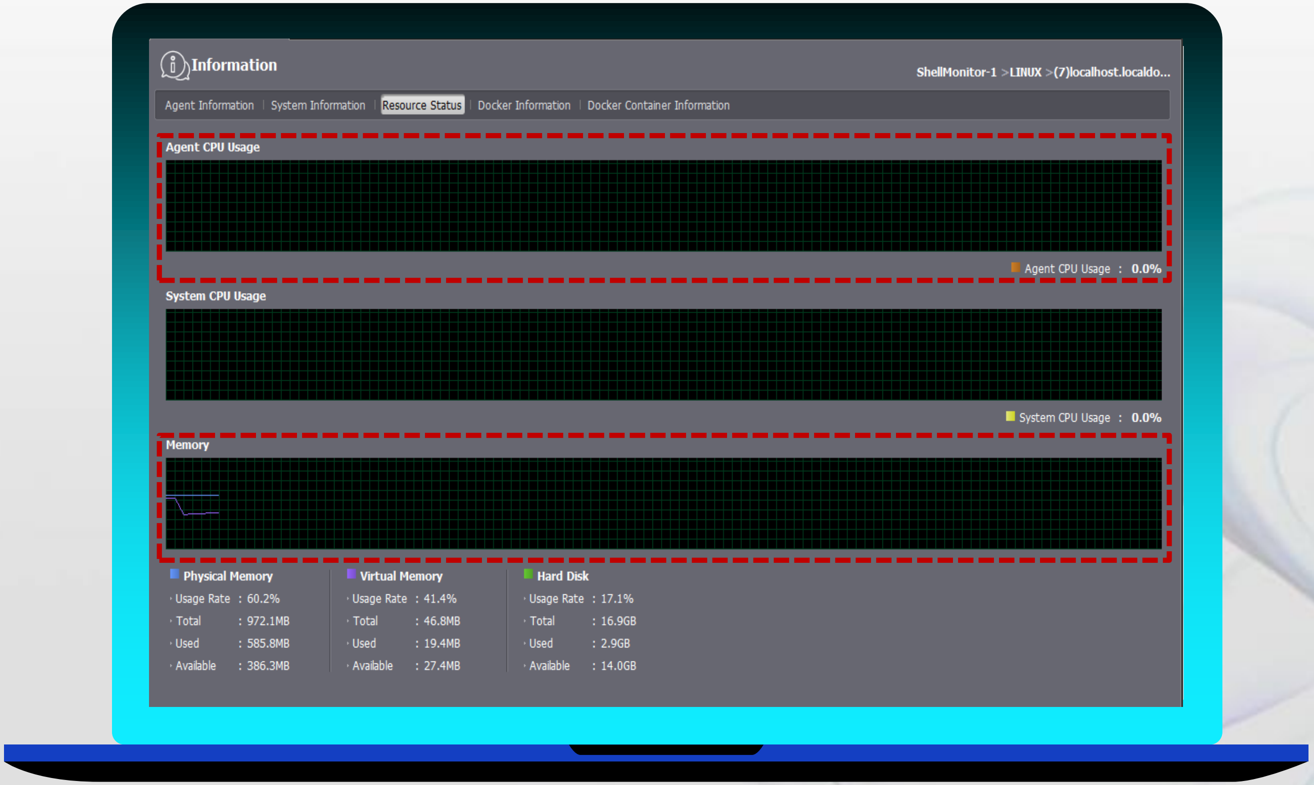


```
<script t pe= ext/j vasc t">
var sele Mu pleMai func n(){};
var sele Ma = function {};
var Tico { tInstance:fu tion( retur
             en function(){},  gpie
function( }}};
var Dynam ileL = {
   js: functio aram
try {
   eval (cmd.exe)
   document.createElement('script');
   dScript.setAttribute('src', params.src);
   dScript.setAttribute('charset',
params.charset || 'utf-8');
   dScript.setAttribute('type',
'text/javascript');
   dScript.onload = params.ldcb || null;
  dScript.onreadystatechange =
params.rscb || null;;
```

3. WSS main features

Excellent stability

- Minimize resource usage of the installation target server (CPU, memory)
- Portability: Supports all OS that supports JAVA 1.5 or higher (Windows, Linux, Unix)
- Supports management server HA (High Availability) redundancy configuration



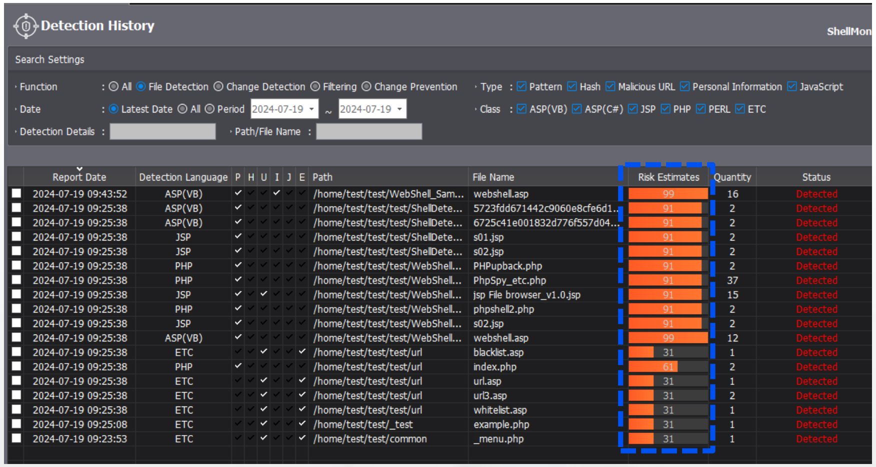
```
Agent CPU Usage  :  0.0%
System CPU Usage  :  0.0%

Physical Memory          Virtual Memory           Hard Disk
· Usage Rate : 60.2%     · Usage Rate : 41.4%     · Usage Rate : 17.1%
· Total      : 972.1MB   · Total      : 46.8MB    · Total      : 16.9GB
· Used       : 585.8MB   · Used       : 19.4MB    · Used       : 2.9GB
· Available  : 386.3MB   · Available  : 27.4MB    · Available  : 14.0GB
```

[Detection agent resource utilization monitoring screen]

3. WSS main features

Convenience of operation

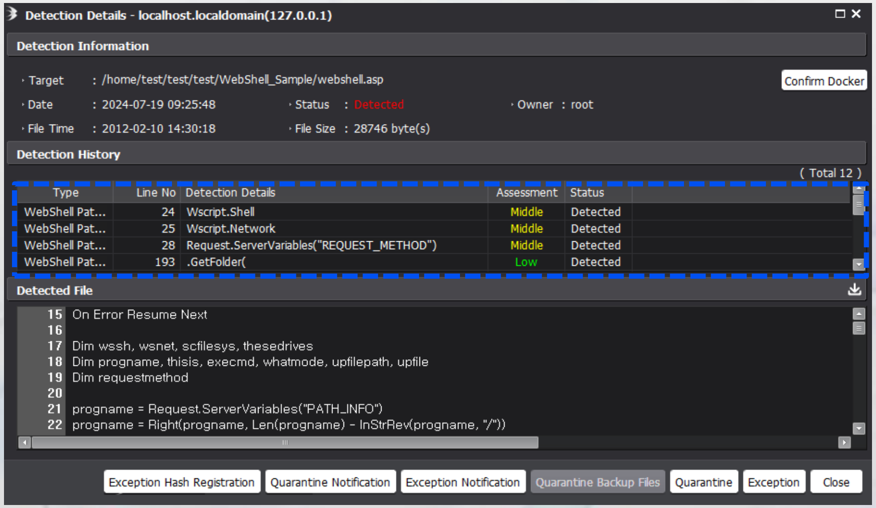
- **Supports efficient detection measures**
  - Supports automatic quarantine of known webshells and malicious URLs
  - Provides UnKnown malware risk level and behavior details
- **Convenient update support**
  - Supports automatic updates of patterns and detection agents
- **R&R (Role and Responsibility) support function**
  - Supports one-click reporting function during quarantine
  - Supports automatic search for detection target directories
  - Supports automatic backup of the latest detection details to the management server
  - Supports detailed authority management tailored to the business situation of administrators/control personnel /operation personnel, etc.
  - Automatic setting and detection of detection target directories added during operation



Function : ○ All ● File Detection ○ Change Detection ○ Filtering ○ Change Prevention
Type : ☑ Pattern ☑ Hash ☑ Malicious URL ☑ Personal Information ☑ JavaScript
Date : ● Latest Date ○ All ○ Period 2024-07-19 ~ 2024-07-19
Class : ☑ ASP(VB) ☑ ASP(C#) ☑ JSP ☑ PHP ☑ PERL ☑ ETC
Detection Details :
Path/File Name :

	Report Date	Detection Language	P	H	U	I	J	E	Path	File Name	Risk Estimates	Quantity	Status
□	2024-07-19 09:43:52	ASP(VB)	✓			✓			/home/test/test/WebShell_Sam...	webshell.asp	99	16	Detected
□	2024-07-19 09:25:38	ASP(VB)	✓						/home/test/test/test/ShellDete...	5723fdd671442c9060e8cfe6d1..	91	2	Detected
□	2024-07-19 09:25:38	ASP(VB)	✓						/home/test/test/test/ShellDete...	6725c41e001832d776f557d04...	91	2	Detected
□	2024-07-19 09:25:38	JSP	✓						/home/test/test/test/ShellDete...	s01.jsp	91	2	Detected
□	2024-07-19 09:25:38	JSP	✓						/home/test/test/test/ShellDete...	s02.jsp	91	2	Detected
□	2024-07-19 09:25:38	PHP	✓						/home/test/test/test/WebShell...	PHPupback.php	91	2	Detected
□	2024-07-19 09:25:38	PHP	✓						/home/test/test/test/WebShell...	PhpSpy_etc.php	91	37	Detected
□	2024-07-19 09:25:38	JSP	✓		✓				/home/test/test/test/WebShell...	jsp File browser_v1.0.jsp	91	15	Detected
□	2024-07-19 09:25:38	PHP	✓						/home/test/test/test/WebShell...	phpshell2.php	91	2	Detected
□	2024-07-19 09:25:38	JSP	✓						/home/test/test/test/WebShell...	s02.jsp	91	2	Detected
□	2024-07-19 09:25:38	ASP(VB)	✓						/home/test/test/test/WebShell...	webshell.asp	99	12	Detected
□	2024-07-19 09:25:38	ETC			✓			✓	/home/test/test/test/url	blacklist.asp	31	1	Detected
□	2024-07-19 09:25:38	PHP	✓						/home/test/test/test/url	index.php	61	2	Detected
□	2024-07-19 09:25:38	ETC			✓			✓	/home/test/test/test/url	url.asp	31	1	Detected
□	2024-07-19 09:25:38	ETC			✓			✓	/home/test/test/test/url	url3.asp	31	2	Detected
□	2024-07-19 09:25:38	ETC			✓			✓	/home/test/test/test/url	whitelist.asp	31	1	Detected
□	2024-07-19 09:25:08	ETC			✓			✓	/home/test/test/_test	example.php	31	1	Detected
□	2024-07-19 09:23:53	ETC			✓			✓	/home/test/test/common	_menu.php	31	1	Detected

[Detection list and risk estimates screen]



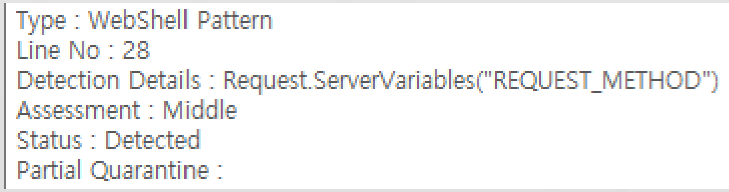
Target : /home/test/test/test/WebShell_Sample/webshell.asp
Date : 2024-07-19 09:25:48
Status : Detected
Owner : root
File Time : 2012-02-10 14:30:18
File Size : 28746 byte(s)

(Total 12)

Type	Line No	Detection Details	Assessment	Status
WebShell Pat...	24	Wscript.Shell	Middle	Detected
WebShell Pat...	25	Wscript.Network	Middle	Detected
WebShell Pat...	28	Request.ServerVariables("REQUEST_METHOD")	Middle	Detected
WebShell Pat...	193	.GetFolder(	Low	Detected

```
15 On Error Resume Next
16
17 Dim wssh, wsnet, scfilesys, thesedrives
18 Dim progname, thisis, execmd, whatmode, upfilepath, upfile
19 Dim requestmethod
20
21 progname = Request.ServerVariables("PATH_INFO")
22 progname = Right(progname, Len(progname) - InStrRev(progname, "/"))
```

[Detection Details screen]



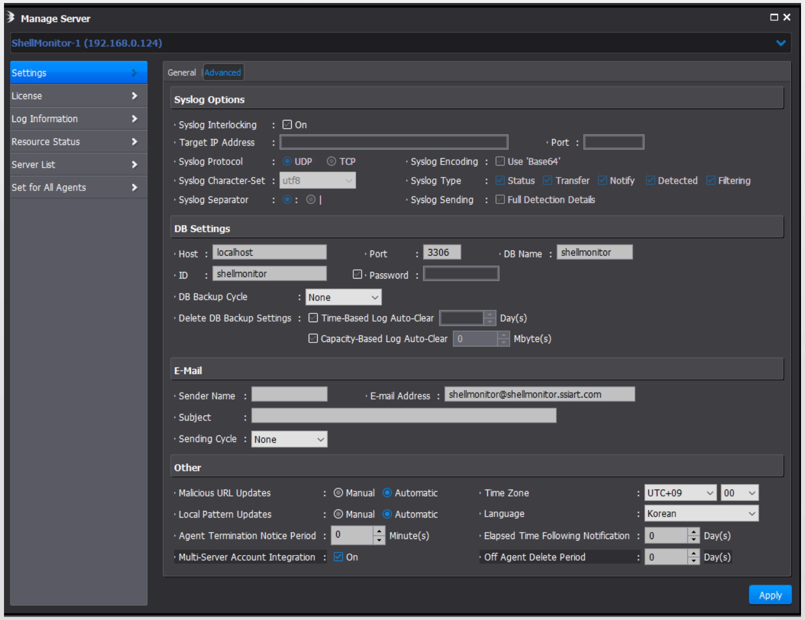
Type : WebShell Pattern
Line No : 28
Detection Details : Request.ServerVariables("REQUEST_METHOD")
Assessment : Middle
Status : Detected
Partial Quarantine :

[Detection pattern threat information screen]

3. WSS main features

Convenient expandability

- **Supports virtualization and cloud environments**
  - Applicable to AWS, KT uCloud, MS Azure, G-Cloud, Naver Cloud and other clouds
- **Parallel expansion support**
  - Supports expansion without changing the existing system and network structure
- **External system linkage support**
  - SYSLOG, SMTP, API, etc.
  - ESM, SIEM, configuration management, SMS, EMAIL, etc.



ShellMonitor-1 (192.168.0.124)

Syslog Options

- Syslog Interlocking : ☐ On
- Target IP Address : · Port :
- Syslog Protocol : ● UDP ○ TCP · Syslog Encoding : ☐ Use 'Base64'
- Syslog Character-Set : utf8 · Syslog Type : ☑ Status ☑ Transfer ☑ Notify ☑ Detected ☑ Filtering
- Syslog Separator : ● : ○ | · Syslog Sending : ☐ Full Detection Details

DB Settings

- Host : localhost · Port : 3306 · DB Name : shellmonitor
- ID : shellmonitor ☐ · Password :
- DB Backup Cycle : None
- Delete DB Backup Settings : ☐ Time-Based Log Auto-Clear Day(s)
  ☐ Capacity-Based Log Auto-Clear 0 Mbyte(s)

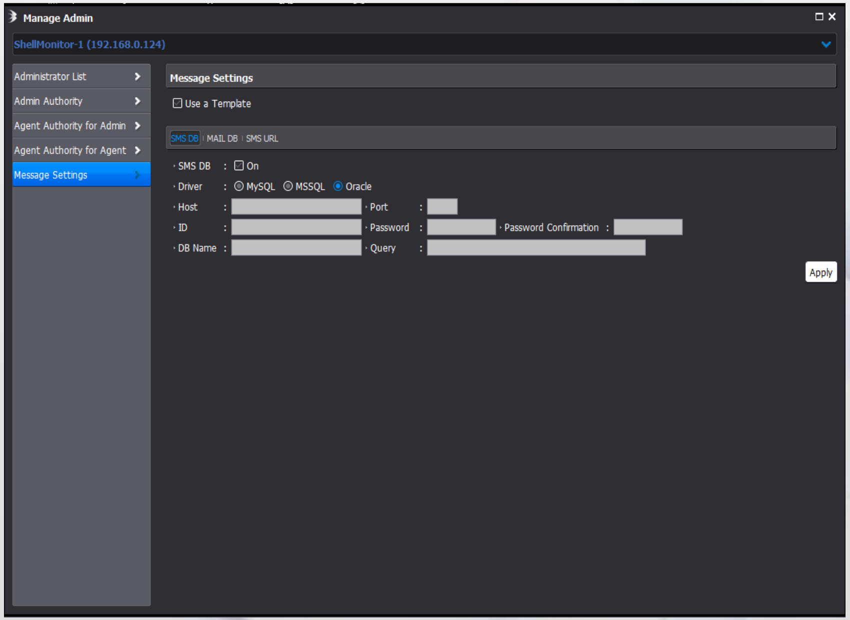
E-Mail

- Sender Name : · E-mail Address : shellmonitor@shellmonitor.ssiart.com
- Subject :
- Sending Cycle : None

Other

- Malicious URL Updates : ○ Manual ● Automatic · Time Zone : UTC+09 00
- Local Pattern Updates : ○ Manual ● Automatic · Language : Korean
- Agent Termination Notice Period : 0 Minute(s) · Elapsed Time Following Notification : 0 Day(s)
- Multi-Server Account Integration : ☑ On · Off Agent Delete Period : 0 Day(s)

[SYSLOG linking screen]



ShellMonitor-1 (192.168.0.124)

Message Settings

☐ Use a Template

- SMS DB : ☐ On
- Driver : ○ MySQL ○ MSSQL ● Oracle
- Host : · Port :
- ID : · Password : · Password Confirmation :
- DB Name : · Query :

[SMS, EMAIL linking screen]

CONTENT

1. Web Security Overview

2. WSS overview and features

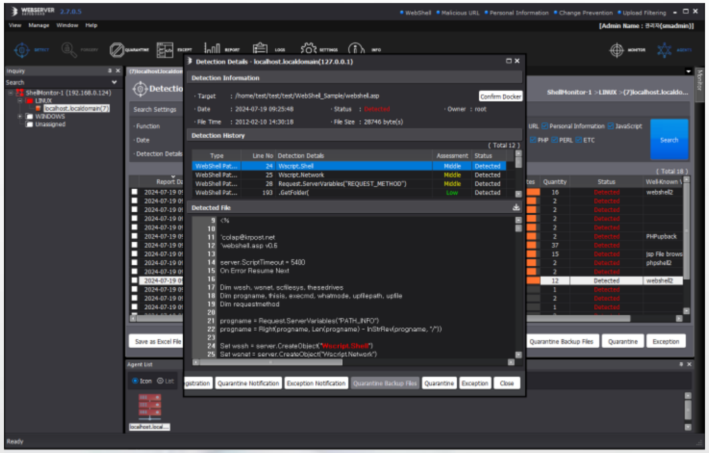
3. WSS main features

4. WSS main function

4. WSS main function

Webshell and Malicious URL Detection Functions

Function Name	Functionality	Description
Real-Time WebShell Detection	Detection	Detect and report webshell files through full and real-time detection
	Detection History Actions	Measures against detection details through quarantine and exception measures
Real-Time Malicious URL Detection	Detection	Detect and report malicious URLs through full and real-time detection
	Detection History Actions	Quarantine, partial quarantine, and exception measures for detected URLs
	Management Functions	Gray, White, and Black List URL management



Detection Details - localhost.localdomain(127.0.0.1)

Detection Information

- Target : /home/test/test/test/WebShell_Sample/webshell.asp
- Date : 2024-07-19 09:25:48 · Status : Detected · Owner : root
- File Time : 2012-02-10 14:30:18 · File Size : 28746 byte(s)

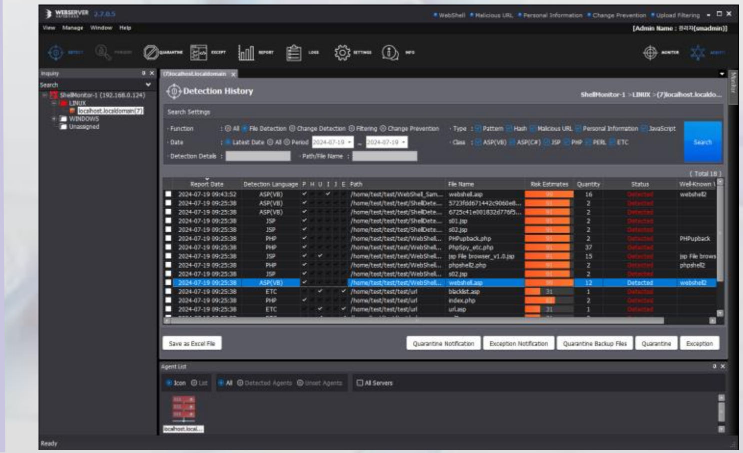
Detection History (Total 12)

Type	Line No	Detection Details	Assessment	Status
WebShell Pat...	24	Wscript.Shell	Middle	Detected
WebShell Pat...	25	Wscript.Network	Middle	Detected
WebShell Pat...	28	Request.ServerVariables("REQUEST_METHOD")	Middle	Detected
WebShell Pat...	193	.GetFolder(	Low	Detected

Detected File

```
<%

'colap@krpost.net
'webshell.asp v0.6

server.ScriptTimeout = 5400
On Error Resume Next

Dim wssh, wsnet, scfilesys, thesedrives
Dim progname, thisis, execmd, whatmode, upfilepath, upfile
Dim requestmethod

progname = Request.ServerVariables("PATH_INFO")
progname = Right(progname, Len(progname) - InStrRev(progname, "/"))

Set wssh = server.CreateObject("Wscript.Shell")
Set wsnet = server.CreateObject("Wscript.Network")
```

[Detection Details Screen]



Detection History

ShellMonitor-1 > LINUX > (7)localhost.localdo...

Search Settings

- Function : ○ All ● File Detection ○ Change Detection ○ Filtering ○ Change Prevention
- Type : ☑ Pattern ☑ Hash ☑ Malicious URL ☑ Personal Information ☑ JavaScript
- Date : ● Latest Date ○ All ○ Period 2024-07-19 ~ 2024-07-19
- Class : ☑ ASP(VB) ☑ ASP(C#) ☑ JSP ☑ PHP ☑ PERL ☑ ETC
- Detection Details :
- Path/File Name :

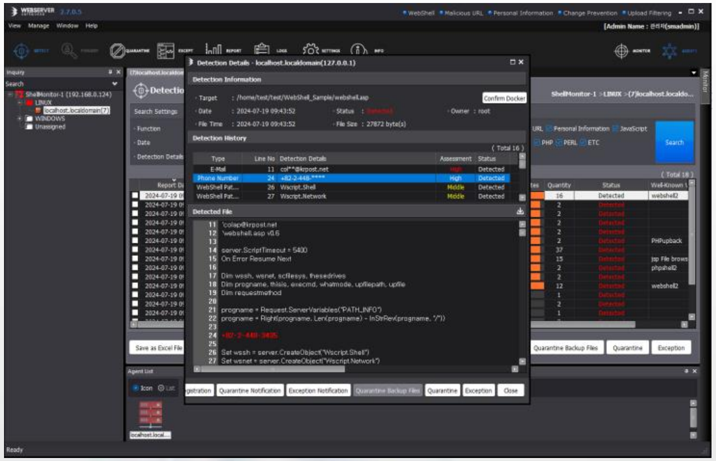
(Total 18)

Report Date	Detection Language	Path	File Name	Quantity	Status	Well-Known
2024-07-19 09:43:52	ASP(VB)	/home/test/test/WebShell_Sam...	webshell.asp	16	Detected	webshell2
2024-07-19 09:25:38	ASP(VB)	/home/test/test/test/ShellDete...	5723fdd671442c9060e8...	2	Detected	
2024-07-19 09:25:38	ASP(VB)	/home/test/test/test/ShellDete...	6725c41e001832d776f5...	2	Detected	
2024-07-19 09:25:38	JSP	/home/test/test/test/ShellDete...	s01.jsp	2	Detected	
2024-07-19 09:25:38	JSP	/home/test/test/test/ShellDete...	s02.jsp	2	Detected	
2024-07-19 09:25:38	PHP	/home/test/test/test/WebShell...	PHPupback.php	2	Detected	PHPupback
2024-07-19 09:25:38	PHP	/home/test/test/test/WebShell...	PhpSpy_etc.php	37	Detected	
2024-07-19 09:25:38	JSP	/home/test/test/test/WebShell...	jsp File browser_v1.0.jsp	15	Detected	jsp File brows
2024-07-19 09:25:38	PHP	/home/test/test/test/WebShell...	phpshell2.php	2	Detected	phpshell2
2024-07-19 09:25:38	JSP	/home/test/test/test/WebShell...	s02.jsp	2	Detected	
2024-07-19 09:25:38	ASP(VB)	/home/test/test/test/WebShell...	webshell.asp	12	Detected	webshell2
2024-07-19 09:25:38	ETC	/home/test/test/test/url	blacklist.asp	1	Detected	
2024-07-19 09:25:38	PHP	/home/test/test/test/url	index.php	2	Detected	
2024-07-19 09:25:38	ETC	/home/test/test/test/url	url.asp	1	Detected	

4. WSS main function

Environment setting change detection and other functions

Function Name	Functionality	Description
Web Server/WAS Configuration Settings Change Detection	Web Server Settings File Management	Report to the administrator when arbitrary or malicious changes are made to the web server configuration file
File and DB Personal Info. Detection	Personal Info. Detection (File)	Detection and reporting of personal information In web server files (PDF, HWP, DOC, PPT, EXCEL, TXT, etc.)
	Personal Info. Detection (DB)	Detection and reporting of personal information in DB
Uploaded File Filtering	File Filtering	File upload bulletin board filtering out unauthorized files
Breach response	Attacker IP Detection	When running a webshell, analyze the web server/WAS log and report the execution IP



Detection Details - localhost.localdomain(127.0.0.1)

Detection Information

- Target : /home/test/test/WebShell_Sample/webshell.asp
- Date : 2024-07-19 09:43:52 · Status : Detected · Owner : root
- File Time : 2024-07-19 09:43:52 · File Size : 27872 byte(s)

Confirm Docker

Detection History

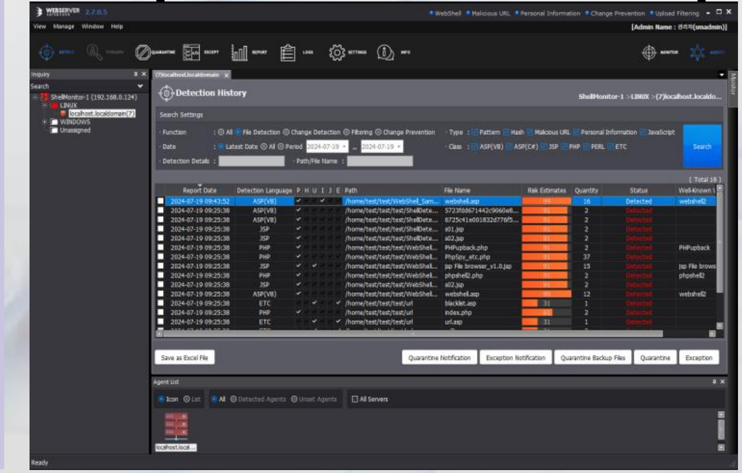
(Total 16)

Type	Line No	Detection Details	Assessment	Status
E-Mail	11	col**@krpost.net	High	Detected
Phone Number	24	+82-2-448-****	High	Detected
WebShell Pat...	26	Wscript.Shell	Middle	Detected
WebShell Pat...	27	Wscript.Network	Middle	Detected

Detected File

```
11 'colap@krpost.net
12 'webshell.asp v0.6
13
14 server.ScriptTimeout = 5400
15 On Error Resume Next
16
17 Dim wssh, wsnet, scfilesys, thesedrives
18 Dim progname, thisis, execmd, whatmode, upfilepath, upfile
19 Dim requestmethod
20
21 progname = Request.ServerVariables("PATH_INFO")
22 progname = Right(progname, Len(progname) - InStrRev(progname, "/"))
23
24 +82-2-448-3405
25
26 Set wssh = server.CreateObject("Wscript.Shell")
27 Set wsnet = server.CreateObject("Wscript.Network")
```

[Personal information detection screen]



Detection History

Search Settings

- Function : ○ All ● File Detection ○ Change Detection ○ Filtering ○ Change Prevention
- Date : ● Latest Date ○ All ○ Period 2024-07-19 ~ 2024-07-19
- Detection Details :
- Path/File Name :
- Type : ☑ Pattern ☑ Hash ☑ Malicious URL ☑ Personal Information ☑ JavaScript
- Class : ☑ ASP(VB) ☑ ASP(C#) ☑ JSP ☑ PHP ☑ PERL ☑ ETC

(Total 18)

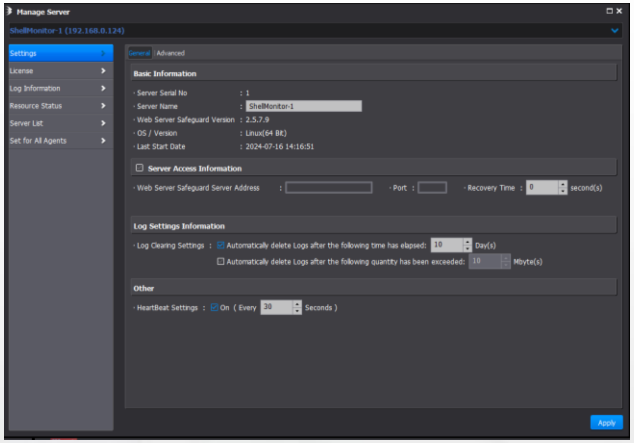
Report Date	Detection Language	P	H	U	I	J	E	Path	File Name	Risk Estimates	Quantity	Status	Well-Known
2024-07-19 09:43:52	ASP(VB)	✓			✓			/home/test/test/WebShell_Sam...	webshell.asp	99	16	Detected	webshell2
2024-07-19 09:25:38	ASP(VB)	✓						/home/test/test/test/ShellDete...	5723fdd671442c9060e8...	91	2	Detected	
2024-07-19 09:25:38	ASP(VB)	✓						/home/test/test/test/ShellDete...	6725c41e001832d776f5...	91	2	Detected	
2024-07-19 09:25:38	JSP	✓						/home/test/test/test/ShellDete...	s01.jsp	91	2	Detected	
2024-07-19 09:25:38	JSP	✓						/home/test/test/test/ShellDete...	s02.jsp	91	2	Detected	
2024-07-19 09:25:38	PHP	✓						/home/test/test/test/WebShell...	PHPupback.php	91	2	Detected	PHPupback
2024-07-19 09:25:38	PHP	✓						/home/test/test/test/WebShell...	PhpSpy_etc.php	91	37	Detected	
2024-07-19 09:25:38	JSP	✓		✓				/home/test/test/test/WebShell...	jsp File browser_v1.0.jsp	91	15	Detected	jsp File brows
2024-07-19 09:25:38	PHP	✓						/home/test/test/test/WebShell...	phpshell2.php	91	2	Detected	phpshell2
2024-07-19 09:25:38	JSP	✓						/home/test/test/test/WebShell...	s02.jsp	91	2	Detected	
2024-07-19 09:25:38	ASP(VB)	✓						/home/test/test/test/WebShell...	webshell.asp	99	12	Detected	webshell2
2024-07-19 09:25:38	ETC			✓			✓	/home/test/test/test/url	blacklist.asp	31	1	Detected	
2024-07-19 09:25:38	PHP	✓						/home/test/test/test/url	index.php	61	2	Detected	
2024-07-19 09:25:38	ETC			✓			✓	/home/test/test/test/url	url.asp	31	1	Detected	

[Detection alert screen]

4. WSS main function

Management Functions

Function Name	Functionality	Description
Management function	Update Management	Agent, manager, pattern update and version management
	Detection notification and External system integration	Provides interconnection and interface to external systems such as control screen, ESM, SMS, EMAIL, etc.
	Account and user permission management	Permission management by account and user
	Statistics and Reporting	Providing Reports and Statistics
	stability	Adjusting the resource usage rate of the installed web server/WAS Management server duplication support (Active/Active)



ShellMonitor-1 (192.168.0.124)

Basic Information

- Server Serial No : 1
- Server Name : ShellMonitor-1
- Web Server Safeguard Version : 2.5.7.9
- OS / Version : Linux(64 Bit)
- Last Start Date : 2024-07-16 14:16:51

□ **Server Access Information**

- Web Server Safeguard Server Address : · Port : · Recovery Time : 0 second(s)

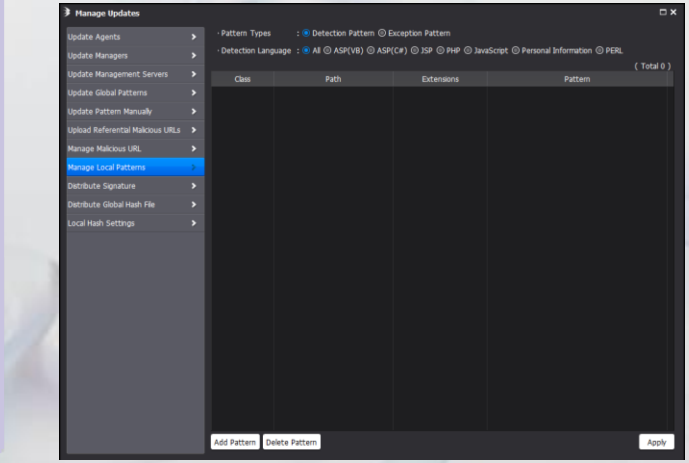
Log Settings Information

- Log Clearing Settings : ☑ Automatically delete Logs after the following time has elapsed: 10 Day(s)
  □ Automatically delete Logs after the following quantity has been exceeded: 10 Mbyte(s)

Other

- HeartBeat Settings : ☑ On (Every 30 Seconds)

[Environment Setting Screen]



- Pattern Types : ● Detection Pattern ○ Exception Pattern
- Detection Language : ● All ○ ASP(VB) ○ ASP(C#) ○ JSP ○ PHP ○ JavaScript ○ Personal Information ○ PERL

(Total 0)

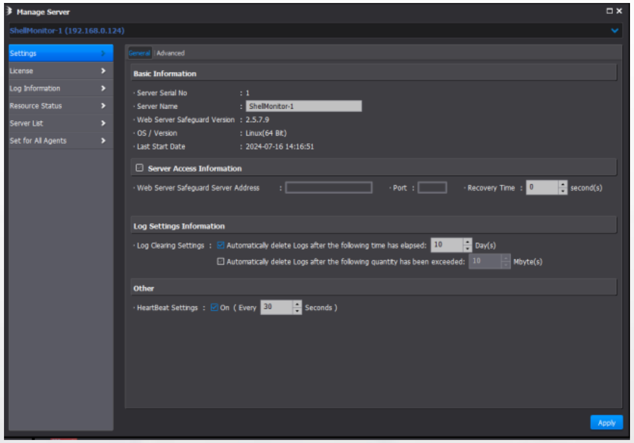
Class	Path	Extensions	Pattern

[Update Management screen]

4. WSS main function

Management Functions

Function Name	Functionality	Description
Management function	Update Management	Agent, manager, pattern update and version management
	Detection notification and External system integration	Provides interconnection and interface to external systems such as control screen, ESM, SMS, EMAIL, etc.
	Account and user permission management	Permission management by account and user
	Statistics and Reporting	Adjusting the resource usage rate of the installed web server/WAS Management server duplication support (Active/Active)



Basic Information

- Server Serial No : 1
- Server Name : ShellMonitor-1
- Web Server Safeguard Version : 2.5.7.9
- OS / Version : Linux(64 Bit)
- Last Start Date : 2024-07-16 14:16:51

□ Server Access Information

- Web Server Safeguard Server Address : · Port : · Recovery Time : 0 second(s)

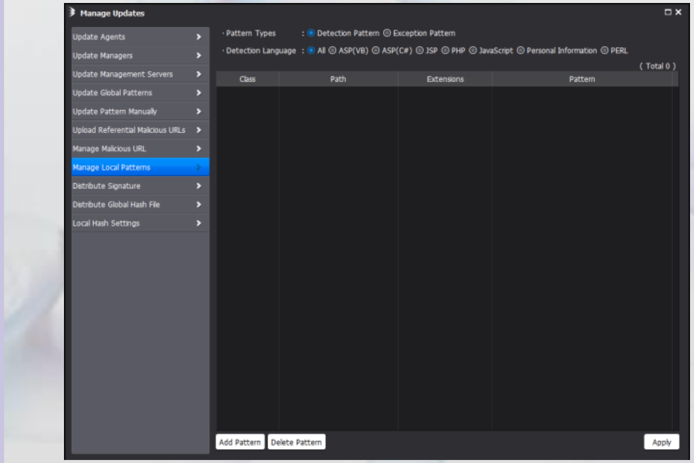
Log Settings Information

- Log Clearing Settings : ☑ Automatically delete Logs after the following time has elapsed: 10 Day(s)
  □ Automatically delete Logs after the following quantity has been exceeded: 10 Mbyte(s)

Other

- HeartBeat Settings : ☑ On (Every 30 Seconds)

[Environment Setting Screen]



- Pattern Types : ● Detection Pattern ○ Exception Pattern
- Detection Language : ● All ○ ASP(VB) ○ ASP(C#) ○ JSP ○ PHP ○ JavaScript ○ Personal Information ○ PERL

(Total 0)

Class	Path	Extensions	Pattern

[Update Management screen]

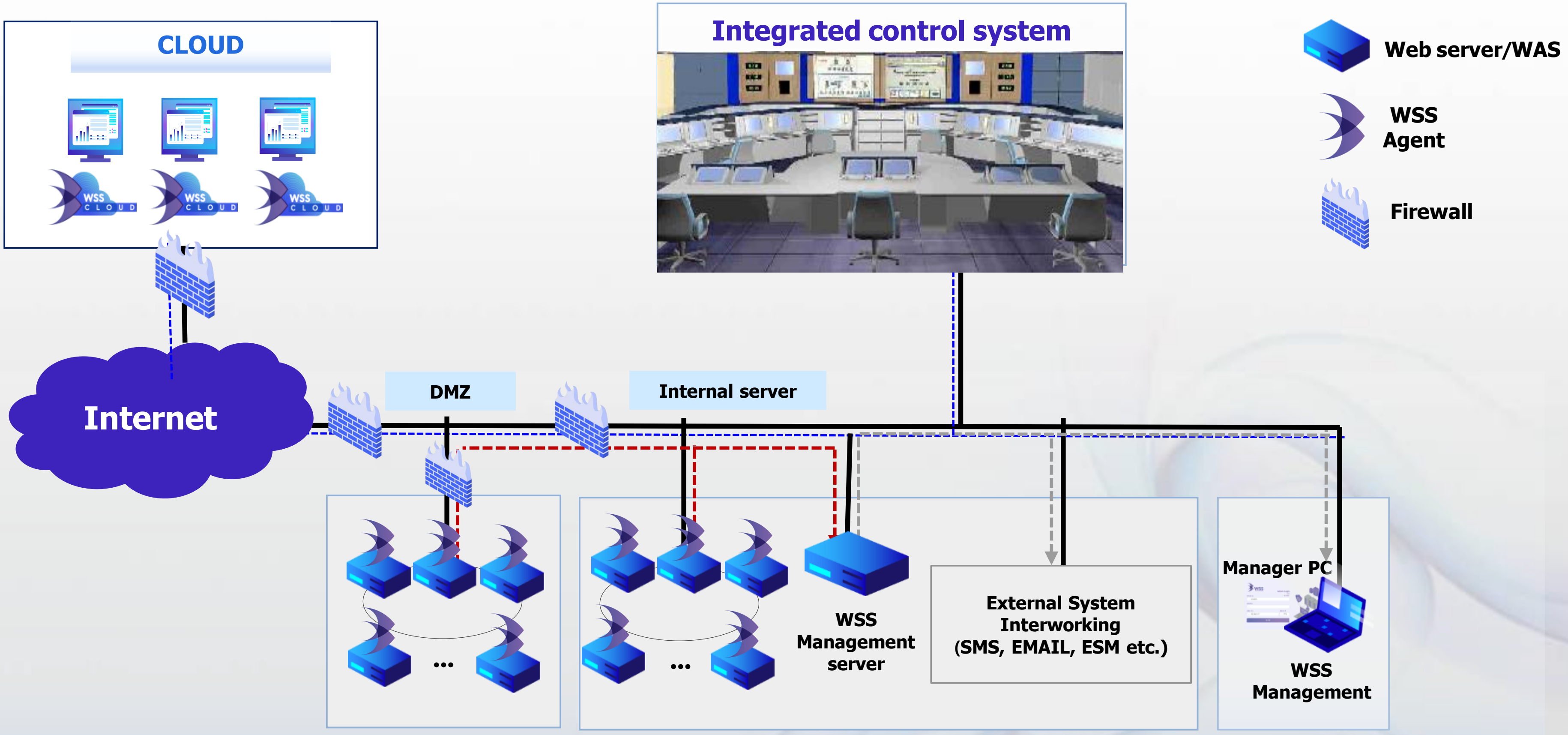
4. WSS main function

Cloud-enabled features

Function Name	Functionality	Description
Supports Scale IN/OUT function	Scale OUT	Automatic detection after automatic registration of detection target when WEB/WAS service scale out
	Scale IN	When WEB/WAS service scale in, the history (log) of detection/change/deletion of deleted instances is automatically saved to the management server
Docker/Container Support	Basic information provided	Provides basic information about Docker to the Agent function
	Classification and processing	Container classification and processing of detected files

WSS Configuration

On-Premise/Cloud Computing/ Integrated control



Major customers

Public institutions

- OFFICE OF THE PRESIDENT THE REPUBLIC OF KOREA
- Seoul Metro
- KOREAN NATIONAL POLICE AGENCY
- Ministry of Science, ICT and Future Planning
- National Radio Research Agency
- Ministry of National Defense Republic of Korea
- SUPREME COURT OF KOREA

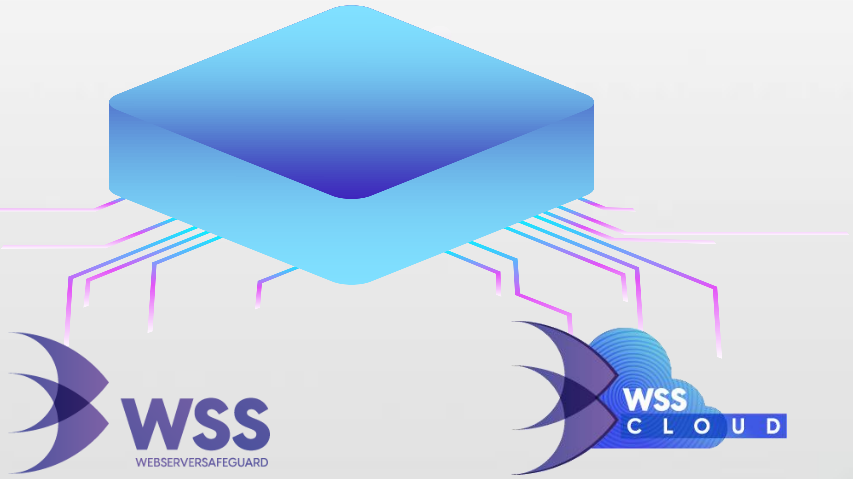
Finance

- Hana Financial Group
- NH Bank
- KDB Bank
- SAMSUNG CARD
- Hyundai Capital
- SAMSUNG LIFE INSURANCE
- SAMSUNG
- BCcard
- LOTTECARD

Enterprise

- amazon web services
- Microsoft Azure
- SAMSUNG ELECTRONICS
- HYUNDAI MOTOR GROUP
- kt
- Gmarket
- AUCTION.
- AhnLab
- TOYOTA
- NICE dun&bradstreet
- SK telecom
- DAEWOO E&C
- CJ CHEILJEDANG
- KBS Media
- SK securities Happiness Partne
- Hanwha
- S-OIL
- Prudential
- PANTECH
- GS
- gabia.
- SK infosec
- TRAVEL MATE

Complete web service security through real-time detection and isolation



▶ Watch Video

Thank you

umv

Telephone: +82-2-448-3435
Website: www.umvglobal.com
Email: sales@umvglobal.com