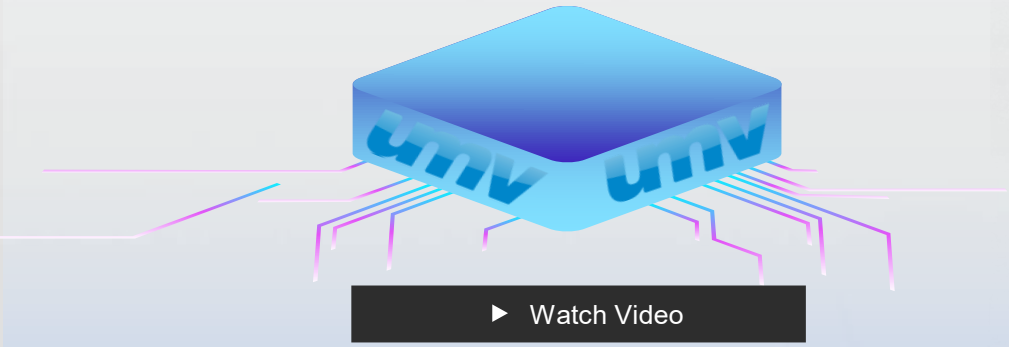
Для интегрированной безопасности веб-сервера и облачной виртуальной машины

WSS (Web Server Safeguard)

Полная безопасность веб-сервисов благодаря обнаружению и изоляции в режиме реального времени



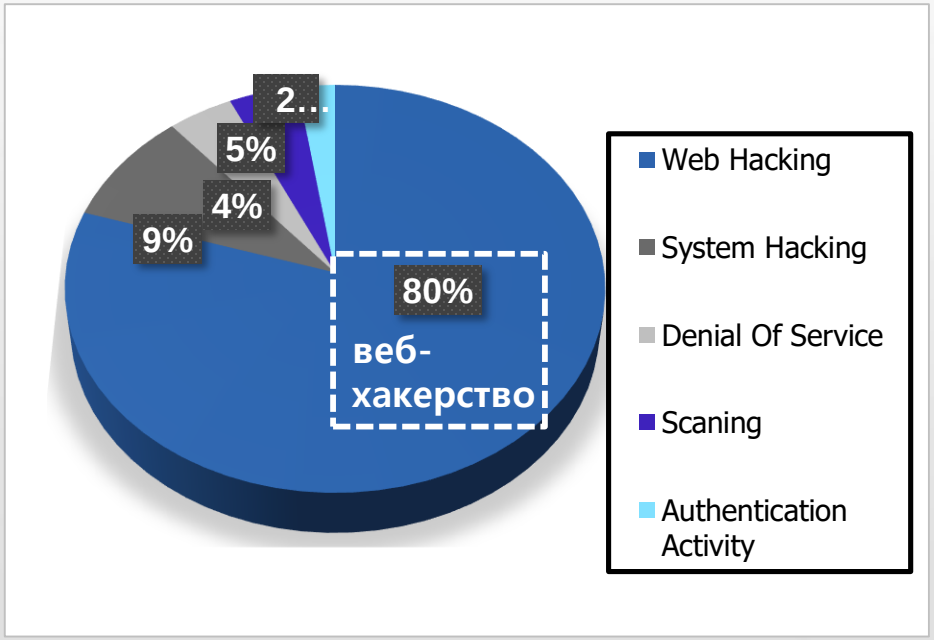
СОДЕРЖАНИЕ

1. Обзор веб-безопасности и ее необходимость

Во всем мире более 80 % кибератак совершается через серверы веб-сервисов, и важность безопасности веб-сервисов растет с каждым днем. С августа 2020 года по январь 2021 года ежемесячно фиксировалось в среднем 140 000 атак с использованием веб-оболочек, и с каждым годом это число увеличивается более чем в два раза.

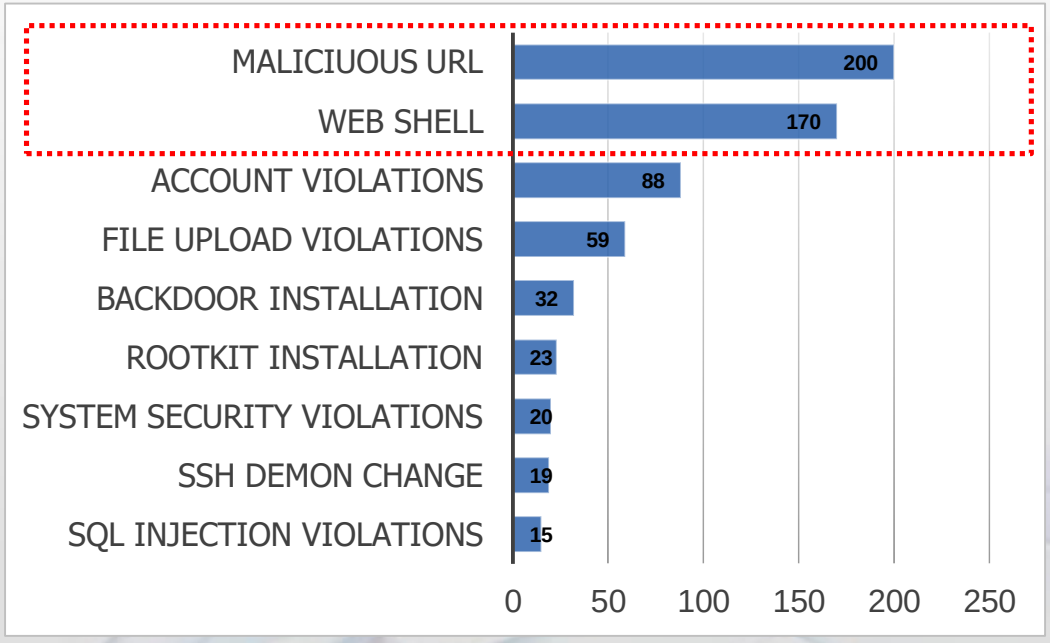
[Источник: Атаки с использованием веб-оболочек продолжают расти, Microsoft security Blog].

КИБЕР АТАКИ



[Источник: KISA Security Control Trend].

ВЕБ-АТАКИ



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

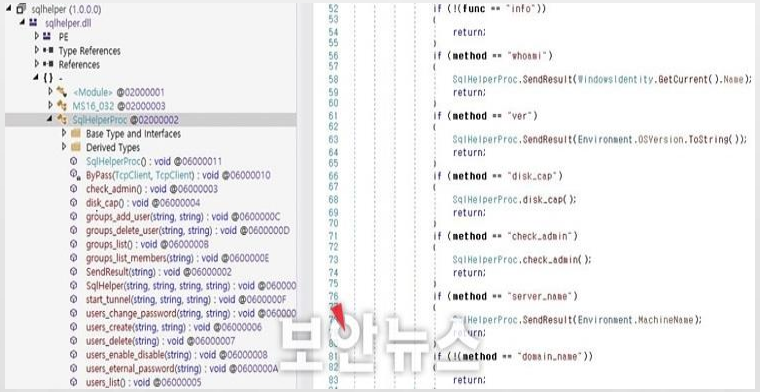
1. Обзор веб-безопасности и ее необходимость

Случай об ущерба от атаки WebShell

Trigona ransomware распространяется через неправильно управляемые серверы MS-SQL

2023-04-12 10:21

Устанавливается не только на серверы Windows, но и в настольные среды... Обнаруживает вредоносное ПО, такое как Remcos RAT. После установки вредоносного ПО CLR Shell приобретаются права администратора, а также устанавливается и заражается программа-вымогатель Trigona. Он регистрирует двоичный файл Trigona в ключе «Выполнить», чтобы его можно было запустить даже после перезагрузки, а затем удаляет тень тома и отключает функцию восстановления системы, что делает восстановление после заражения программой-вымогателем невозможным.



▲ Вредоносная программаCLR Shell, использованная в атаке [Данные = AhnLab ASEC Analysis Team]

Китайская хакерская организация Xiaoqing раскрывает в даркнете личную информацию трех взломанных академических учреждений

2023-01-29 14:27

Личная информация, такая как номер мобильного телефона и адрес, которая выглядит как информация об участниках, раскрывается во внутренних базах данных трех организаций: Корейского археологического общества, Корейского общества по принципам образования и Корейской ассоциации родителей на темном веб-форуме. В том числе... есть вероятность утечки прошлой информации. Команды SQL были отправлены через Интернет, а информация учетной записи веб-администратора, хранящаяся в базе данных, была украдена. (Вставить веб-шелл) Сяоциин украл или удалил внутреннюю информацию компании посредством взлома. Они также превращали веб-сайты в свои собственные веб-страницы или создавали их без разрешения.

◀ Вид веб-страницы, загруженной на сайт, взломанный Xiaoqing/ Фото предоставлено Корейским агентством Интернета и безопасности

1. Обзор веб-безопасности и ее необходимость

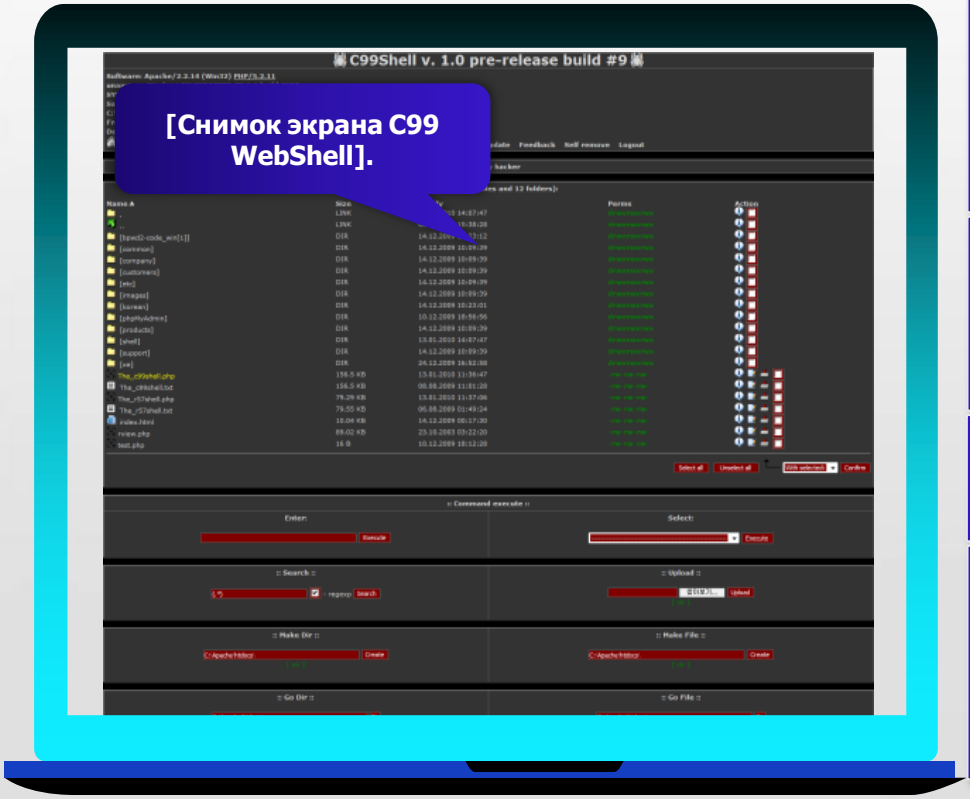
Что такое "вредоносное ПО" или "WebShell"?

- Это программа-инструкция, которая внедряется путем использования уязвимостей в веб-сервере и, будучи выполненной как скрипт на стороне сервера (ASP, JSP, PHP, CGI, PYTHON и т.д.), может получить контроль над сервером, эквивалентный привилегиям root.
- Порты для веб-сервисов (http (80, 8080), https (443)) действуют как бэкдоры и подвержены серьезным хакерским атакам, таким как кража конфиденциальных данных, повреждение веб-страниц и передача доступа к неавторизованным страницам, а также распространение вредоносных программ.

1. Обзор веб-безопасности и ее необходимость

Вредоносные программы на основе веб-технологий/ "Webshell"

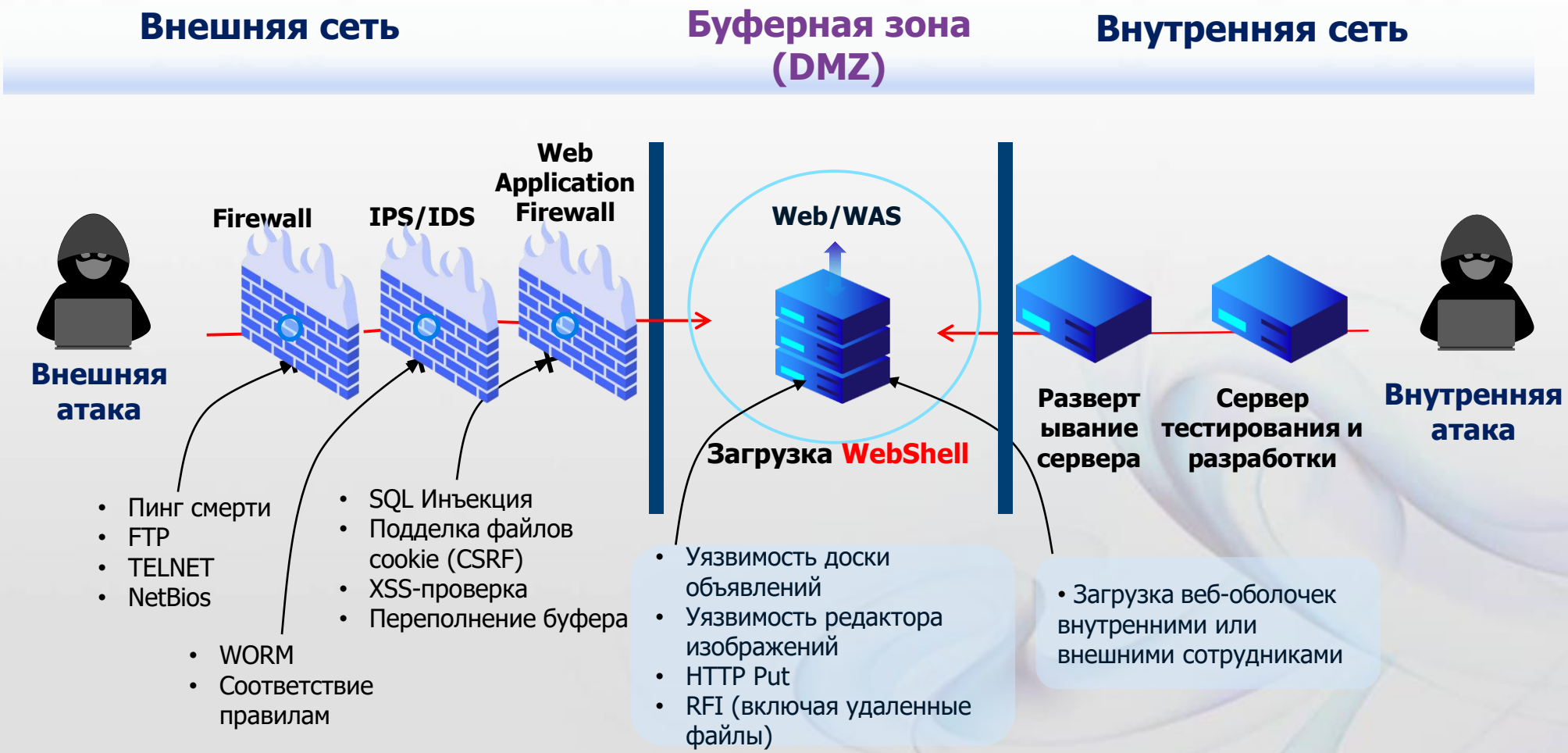
- Webshell обходит системы безопасности и позволяет легко получить доступ к существующим системам без аутентификации.
- Веб-оболочки потенциально опасны, поскольку их сложно обнаружить до момента взлома.



Системное командование	- Просмотр информации о системе - Отключение системы - Остановка/удаление определенных программ - (Пример: антивирусная программа)
Сеть	- Сканер портов - TELNET, SSH, FTP - Доступ (возможен доступ к внутренней сети)
База данных	- Утечка, изменение, удаление данных
Системный файл	- Загрузка инструментов для взлома (кейлог, бэкдор) - Модификация файлов (вставка вредоносного кода) - Удаление системных файлов - Просмотр всех системных каталогов

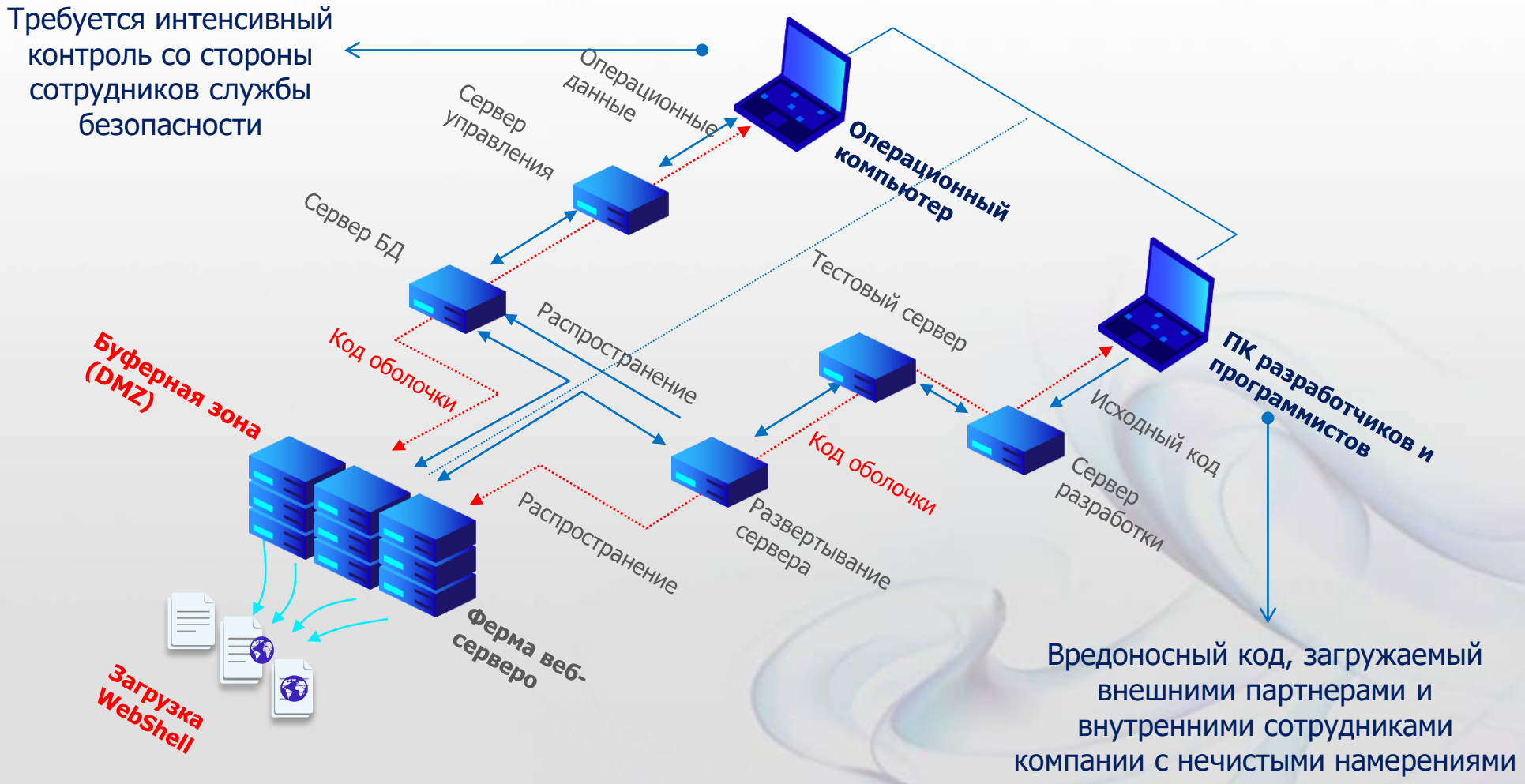
1. Обзор веб-безопасности и ее необходимость

Маршрут проникновения вредоносного кода (WebShell)



Вторжение из внешней сети

Вторжение из внутренней сети



Процесс веб-взлома

В последнее время попытки веб-взлома предпринимаются комплексным и непрерывным образом (APT-атака) на основе веб-оболочек и выполняются шаг за шагом с точной целью атаки.

- **Атака с внедрением URL-адреса вредоносного ПО**
- **Атака с целью порчи домашней страницы**
- **Атаки с подделкой исходного кода и содержимого**

1-я атака

Захват веб-сервера

Анализ уязвимости → **Загрузка Webshell** → Взятие на себя управление веб-сервером → Изменение файла конфигурации веб-сервера (создание уязвимостей)

2-ая атака

Взятие под контроль целевые ПК руководителей/сотрудников

Заражение вредоносным кодом через вредоносный URL → **Zombie PC** → Кража внутреннего идентификатора/пароля сервера управления → Вторжение на внутренний сервер

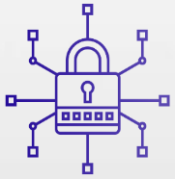
3-я атака

Взятие под контроль внутренний сервер

Вторжение на внутренний сервер → **Кража важной информации** → **РАЗРУШЕНИЕ СИСТЕМЫ**

Тип веб-атаки

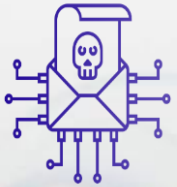
Потенциальные факторы риска, вызванные сотрудниками внутренних и внешних партнеров



Атаки с использованием уязвимостей решений сетевой безопасности

- Уязвимости оборудования сетевой безопасности (анализ по пакетам)
- Атака вредоносного ПО, скомпилированного антивирусом, на основе двоичного кода

Веб-хакинг



Атака на загрузку доски объявлений
Атака на загрузку с использованием уязвимостей исходного кода

- Уязвимость взлома расширения
- Атака, замаскированная под файл изображения

Web server/WAS OS
Атака на уязвимость нулевого дня

Типы веб-атак

Крупные веб-атаки используют уязвимости веб-исходного кода и приводят к модификации исходного кода и данных, которая принимает форму таких атак, как веб-оболочки, вредоносные URL-адреса, подделка домашней страницы и изменение файла конфигурации веб-сервера.

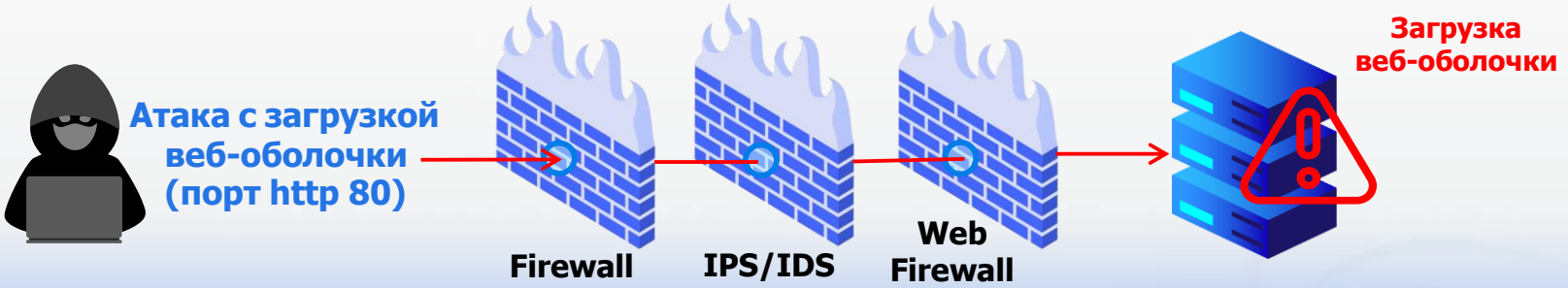
- Атака загрузки веб-шелла
- Атака с использованием вредоносного URL-адреса
- Дефейс-атака на домашнюю страницу
- Атака на файл конфигурации веб-сервера
- Подделка исходного кода и содержимого
- Уязвимости исходного кода

1. Обзор веб-безопасности и ее необходимость

Типы веб-атак

Атака загрузки веб-шелла

После загрузки и выполнения на веб-сервере становится возможным управление сервером, эквивалентное root-правам.

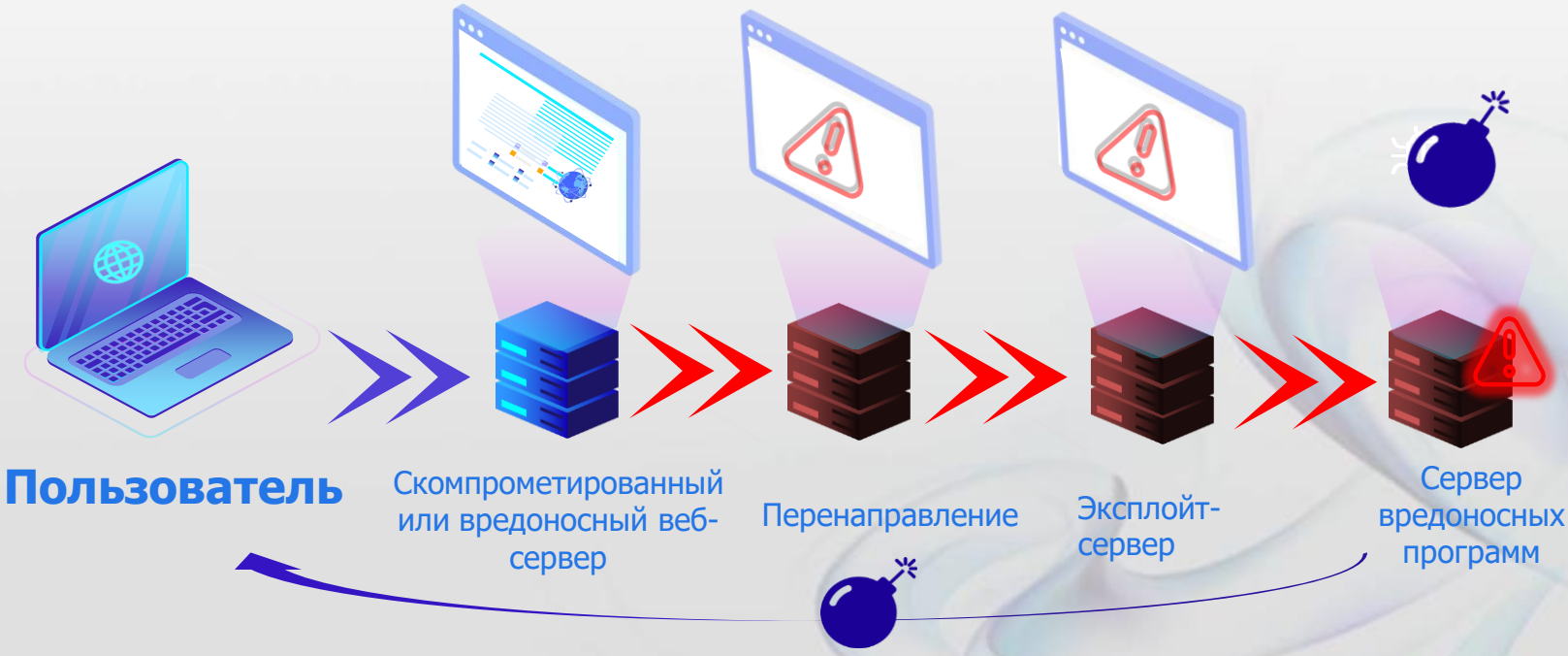


Системные команды	Сетевые команды	Доступ к системным файлам	Доступ к базе данных	Пользовательский ПК
• Просмотр информации о системе • Выключение системы • Остановка/удаление определенной программы (Антивирусное программное обеспечение и т.д.)	• Сканер портов • TELNET, SSH, FTP доступ (доступ к внутренней сети)	• Загрузка инструментов для взлома (кейлог, бэкдор) • Модификация файлов (внедрение вредоносных программ) • Удаление системных файлов • Просмотр системного каталога	• Утечка данных • Изменение данных • Удаление данных	• Заражение вредоносным ПО • Утечка данных • Утечка информации об основном доступе администратора к системе • Провоцирование DDoS-атак

Типы веб-атак

Атака с использованием вредоносных URL-адресов

Вредоносные URL-адреса — это URL-адреса или IP-адреса, которые используют веб-серверы в качестве транзитной точки для вредоносного кода для распространения вирусов, программ- вымогателей и т. д. на компьютеры в больших количествах и могут нанести серьезный ущерб, такой как шифрование файлов, утечка личной информации и DDoS-атаки.



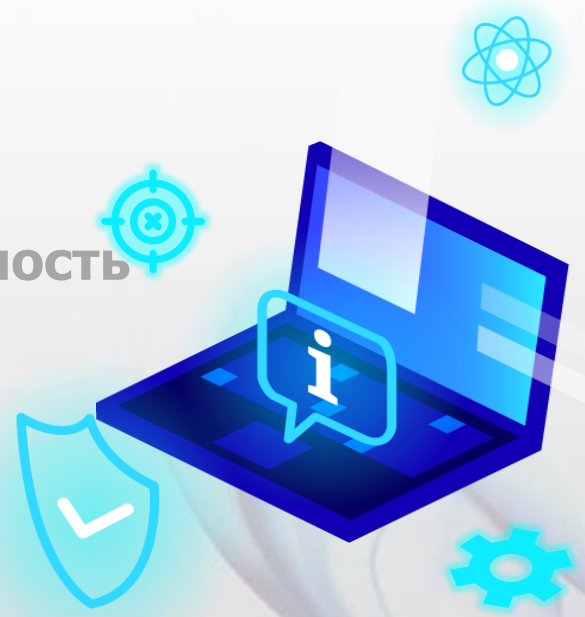
Источник: Аналитический отчет MS Security

Типы веб-атак

Атака с подделкой файла конфигурации веб-сервера

Хакеры изменяют файлы конфигурации веб-сервера, создавая новые уязвимости и используют их в качестве вторичного пути атаки

СОДЕРЖАНИЕ



2. Введение в WSS (обзор и структура)

WSS (Web Server Safeguard)?

WSS — это решение безопасности, специфичное для веб-оболочки, которое обеспечивает безопасную работу веб-серверов путем мониторинга в режиме реального времени «веб-оболочки», вредоносной программы, используемой для взлома веб-сервера.

Обнаружение веб-шеллов и принятие мер к ним

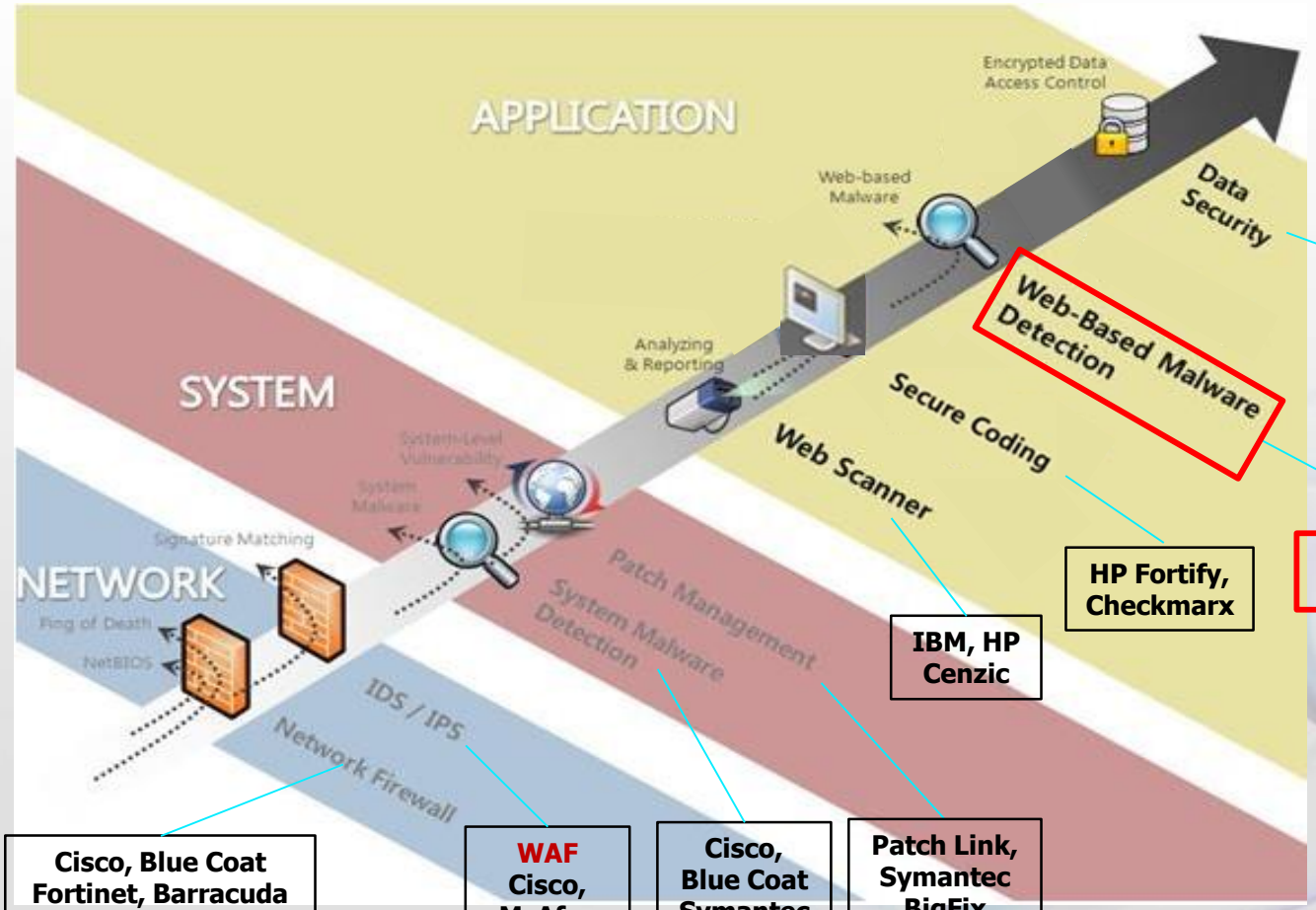
Обнаружение и принятие мер по вредоносным URL-адресам

Предотвращение изменений в файлах конфигурации веб-сервера

Облачные вычисления Поддержка VM, Docker

Позиционирование WSS

Веб-безопасность 3 уровня и решения



2. Введение в WSS (обзор и структура)

Позиционирование WSS

Безопасность WEB-приложений

- **Основой веб-безопасности является безопасность веб-приложений.**
- **Безопасность приложений требует тщательного управления на всех этапах разработки и после развертывания.**

▷ **Веб-сканер**
Программа, которая анализирует уязвимости дизайна и потенциальные уязвимости в веб-приложениях.

▷ **Безопасное кодирование**
При кодировании безопасность учитывается уже на этапе проектирования, чтобы свести к минимуму уязвимости, которые могут возникнуть по различным причинам, таким как недостаток знаний разработчика и ошибки в процессе разработки.

▷ **Обнаружение вредоносных программ на основе веб**
Это решение обнаруживает вредоносное веб-программное обеспечение, называемое «веб-оболочкой», загруженное на веб-серверы. После загрузки веб-оболочки практически трудно обнаружить, и хакеры используют веб-оболочки для различных целей для взлома.

▷ **Безопасность данных**
Это решение обычно хранит данные и создает базу данных в среде веб-приложений, а также безопасно управляет такими данными.

2. Введение в WSS (обзор и структура)

Почему именно WSS (Web Server Safeguard)?

WSS защищает от различных веб-атак хакеров посредством уязвимостей веб- приложений.

* Взаимодополняющие отношения с Web Application Firewall (WAF), устройством сетевой безопасности.

- Существуют ограничения в защите сети из-за диверсификации методов вторжения (возникающая необходимость обнаружения/карантинизации вредоносного ПО веб-сервера внутри системы)
- Рост инцидентов ИБ, вызванных не только внешними взломами, но и действиями пользователей внутри организации
- Невозможно обнаружить вредоносное ПО, проникшее на веб-сервер до установки веб-брандмауэра
- Перегрузка для полных проверок
- Возможность проникновения через уязвимость обхода сети
- Риски шифрования/кодирования трафика и обработки исключений политики безопасности

2. Введение в WSS (обзор и структура)

Обзор и основные характеристики

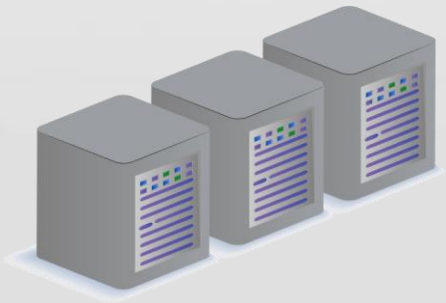
Название продукта	WSS (Web Server Safeguard)
Последняя версия	v2.7
Дата выхода	Май 2010 г.
Производитель	UMV Inc.

- **Обнаружение веб-оболочки**
  - Обнаружение WebShell
  - Карантин
  - Исключение
- **Вредоносный URL**
  - Черный список
  - Белый список
  - Серый список
  - Управление URL/URI
- **Предотвращение изменений в файлах конфигурации веб-сервера**
  - Обнаружение изменений в файлах
  - Предотвращение изменения файлов
- **Функция управления**
  - Управление правами
  - Управление агентами
  - Управление обновлениями
  - Автоматическое нахождение домашнего каталога
- **Функция поддержки облачных систем**
  - Поддержка увеличения/уменьшения масштаба
  - Управление историей
  - Управление сетевой безопасностью
  - Функции поддержки Docker/Container

Настройка решения WSS

Состоит из сервера управления, агента и программы-менеджера (ПК).

Сервер управления WSS	Агент WSS	Менеджерская программа (ПК)
• Серверное ПО, установленное на BM или HW Работает при подключении к WSS Agent • Сохранение истории обнаружения и информации об обнаружении • Удаленный контроль управления • В дополнение к обновлению шаблонов веб-оболочек и развертыванию агентов	• Программа, установленная на веб-сервере/WAS • Обнаружение веб-оболочек и URL-адресов вредоносных программ • Обнаружение веб-оболочек и фильтрация прогресса передачи сервера и т.д. • Поддерживается JDK 1.5 Unix, Linux, NT O/S	• Установка на ПК под управлением администратора (подключение к серверу управления WSS) • Запустить обнаружение веб-оболочки • Мониторинг, удаленные действия, экологические настройки • Управление полномочиями администратора, статистика и отчетность и т.д.



2. Введение в WSS (обзор и структура)

Метод обнаружения WSS

WSS собирает вредоносные программы, чтобы повысить эффективность обнаружения.

- ✓ **Анализ истории обнаружения более 30 000 примененных агентов**
- ✓ **Управление персоналом, специализирующимся на сборе и анализе вредоносного кода**

Обнаружение шаблонов

- Обнаружение шаблонов веб-оболочек путем сравнения шаблонов в обнаруженных файлах с шаблонами в ваших собственных веб-оболочках
- Создание шаблонов веб-оболочек из сигнатур / Обнаружение известных веб-оболочек

Обнаружение хэш-значений

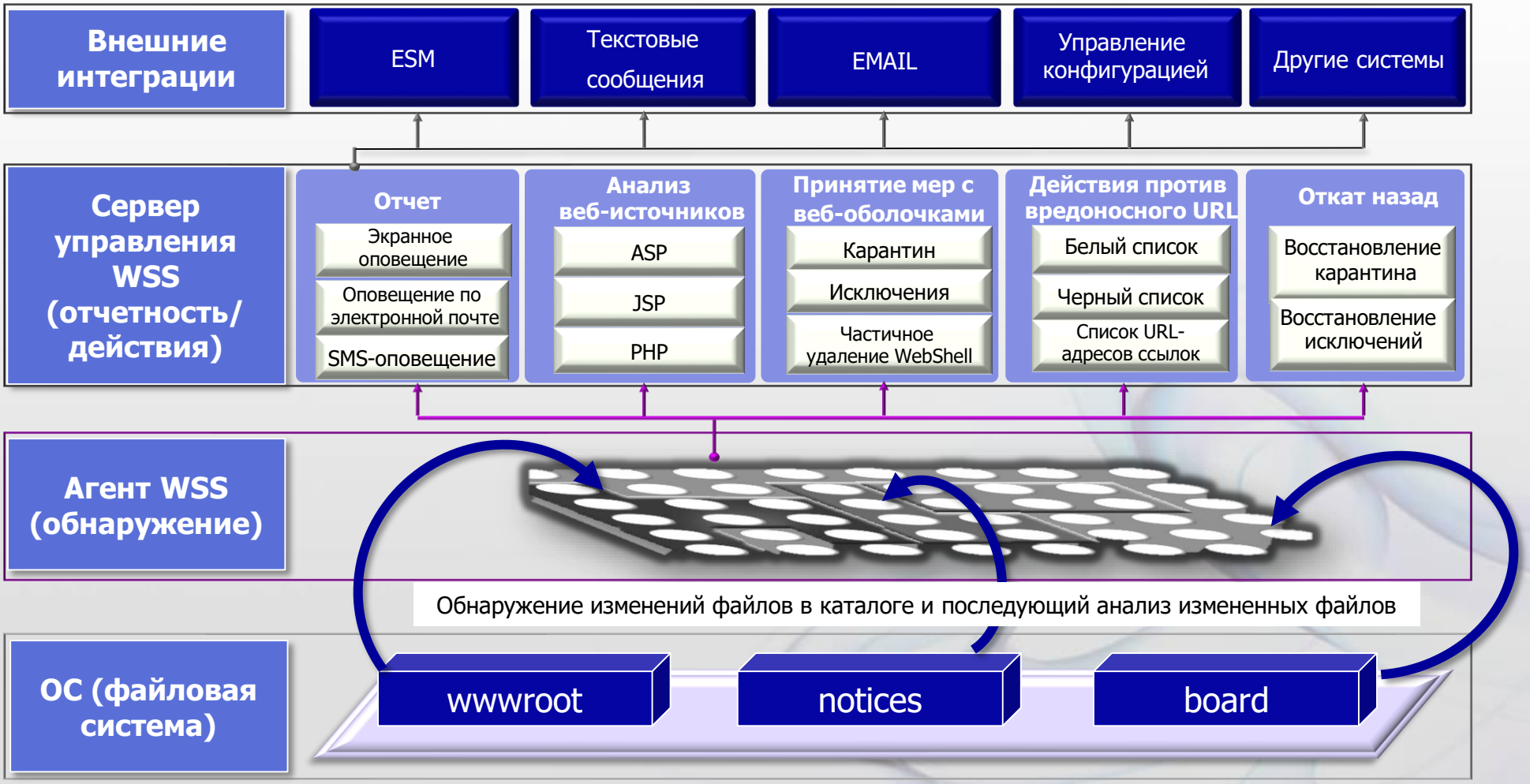
- Если шаблон продолжает увеличиваться, скорость системы снижается. Для эффективной работы WSS обнаруживает периодические обновления хеш-значения www.virustotal.com, портала для обмена вредоносным кодом.

Обнаружение алгоритма

- Обнаруживает запутанные или закодированные веб-оболочки, такие как JAVA Script, через внутренний код.

Структура и принцип работы

Обнаружение вредоносных программ или их создание с помощью мониторинга файловой системы.



СОДЕРЖАНИЕ

3. Основные характеристики WSS

Отличная производительность обнаружения

- WSS поддерживает обнаружение неизвестных вредоносных программ с помощью механизма анализа, предназначенного для обфускации (SCR Parser).
- Сбор вредоносного ПО для повышения эффективности обнаружения.
  - Анализ истории обнаружения агентов, примененный к более чем 30 000 устройств
  - Работа экспертов по сбору и анализу вредоносного кода
- Поддерживает сложное применение шаблонов и обработку исключений для минимизации ложных срабатываний.
- Поддерживает настройку шаблона с учетом среды каждого веб-сервера/WAS

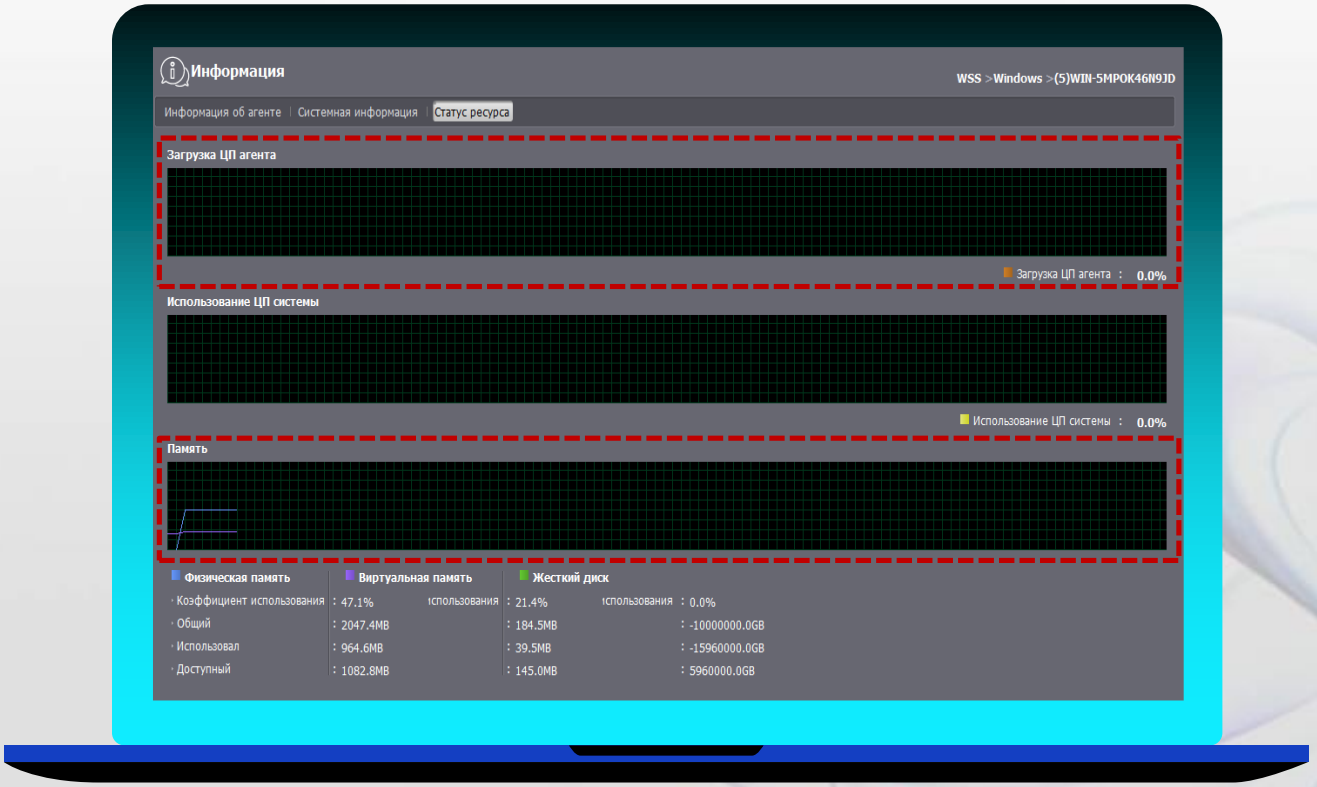
SCR Parser (парсер рекомбинантного исходного кода)

Специальный механизм для анализа и обнаружения обфусцированного исходного кода

3. Основные характеристики WSS

Высокая надежность

- Минимизируйте использование ресурсов целевого сервера установки (процессор, память).
- Портативность: Поддерживает все ОС, поддерживающие JAVA 1.5 или выше (Windows, Linux, Unix).
- Поддержка конфигурации резервирования серверов управления HA (High Availability)

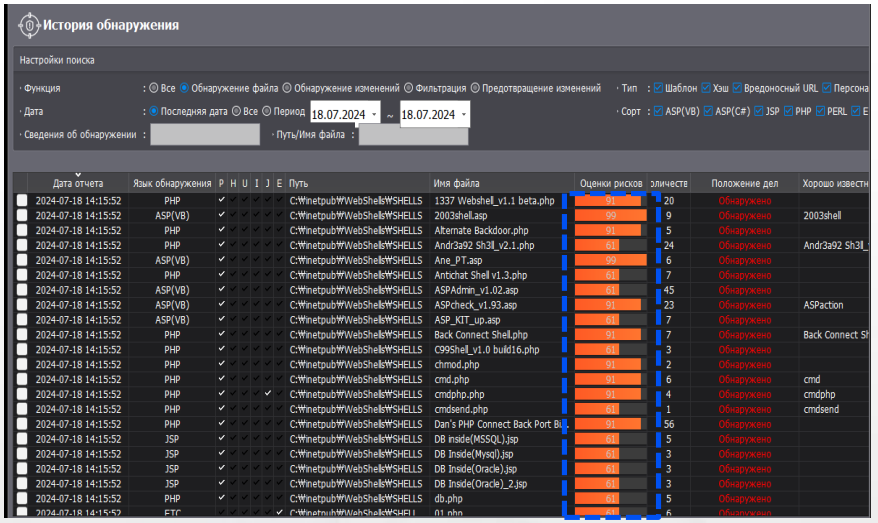


[Экран мониторинга использования ресурсов агента обнаружения]

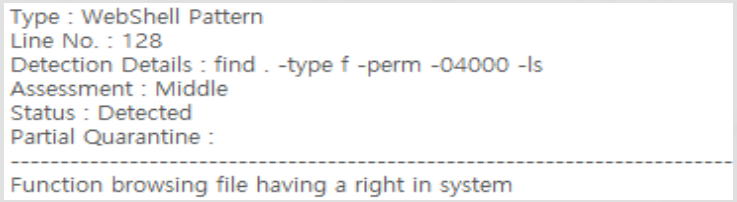
3. Основные характеристики WSS

Удобство эксплуатации

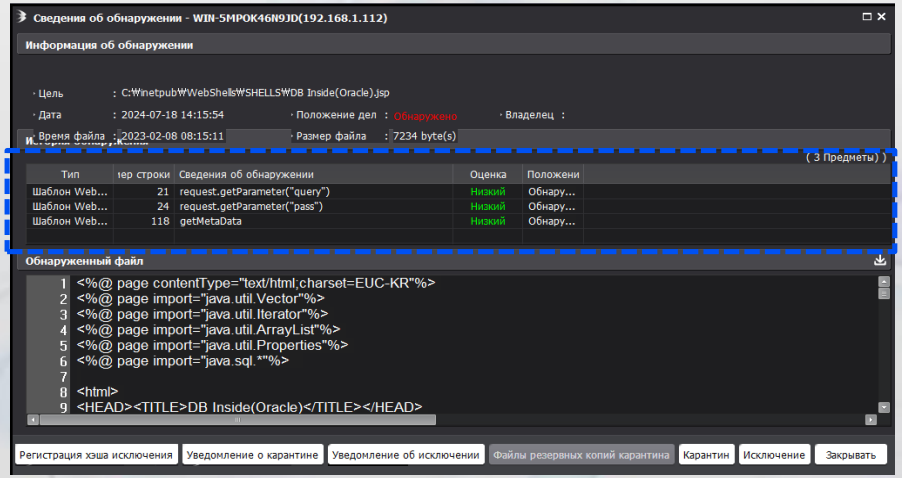
- **Поддерживает эффективные меры обнаружению**
  - Поддерживает автоматический карантин известных веб-оболочек и вредоносных URL-адресов
  - Предоставляет неизвестный уровень риска вредоносного ПО и подробную информацию о поведении.
- **Удобная поддержка обновлений**
  - Поддерживает автоматическое обновление шаблонов и агентов обнаружения
- **Функция поддержки R&R (Роль и ответственность)**
  - Поддерживает функцию отчетности в один клик во время карантина
  - Поддерживает автоматический поиск целевых каталогов обнаружения
  - Поддерживает автоматическое резервное копирование последних сведений об обнаружении на сервер управления.
  - Поддерживает детальное управление полномочиями администраторов/контролирующего персонала/оперативного персонала и т.д. в соответствии с ситуацией в бизнесе.
  - Автоматическая настройка и обнаружение целевых каталогов, добавленных во время работы



[Экран списка обнаружений и информации об оценке риска]



[Экран информации об угрозе шаблона обнаружения]



[Экран подробной информации об обнаружении]

3. Основные характеристики WSS

Удобная возможность расширения

- **Поддержка виртуализации и облачных сред**

- Применимо к AWS, KT uCloud, MS Azure, G-Cloud, Naver Cloud и другим облакам.

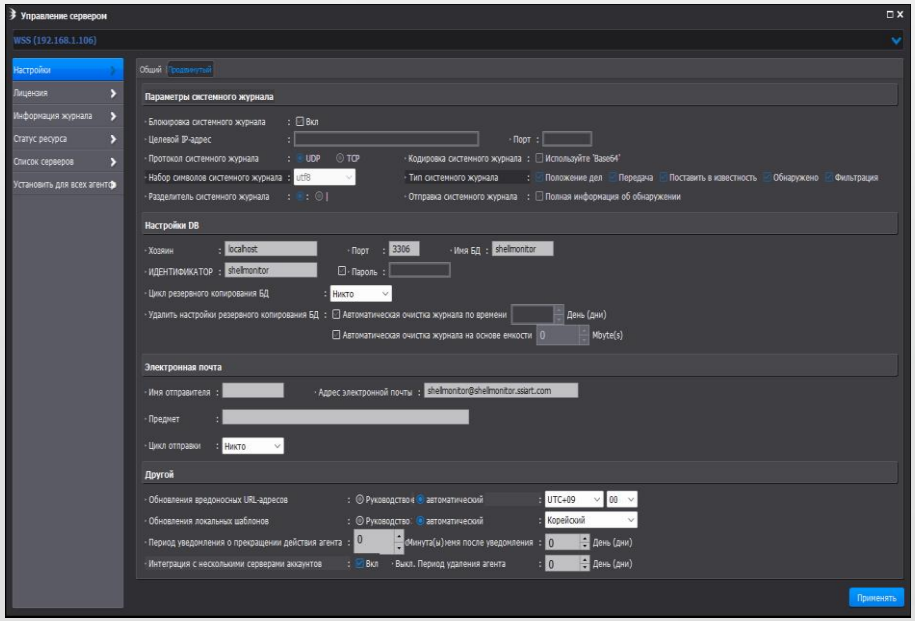
- **Поддержка параллельного расширения**

- Поддержка расширения без изменения существующей системы и структуры сети

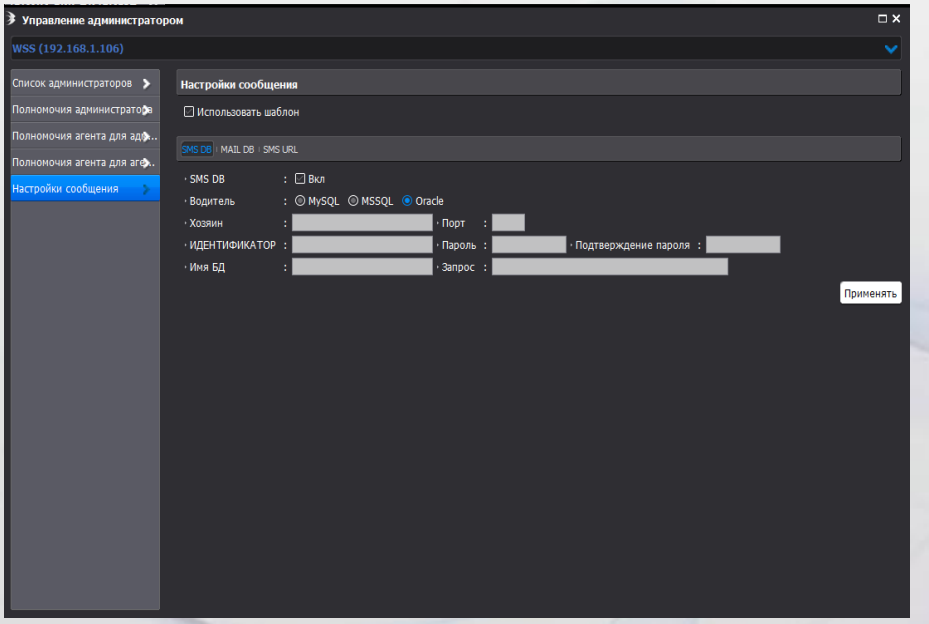
- **Поддержка межсетевого взаимодействия с внешними системами**

- SYSLOG, SMTP, API и т.д.

- ESM, SIEM, управление конфигурацией, SMS, EMAIL и т.д.



[Экран интеграции SYSLOG]



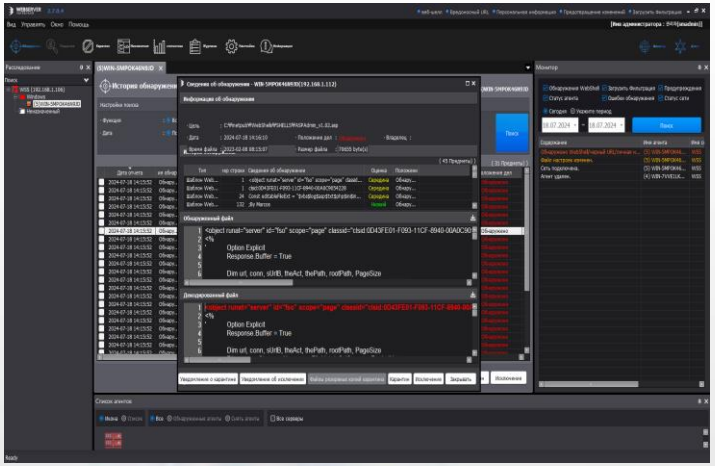
[Экран интеграции SMS, EMAIL]

СОДЕРЖАНИЕ

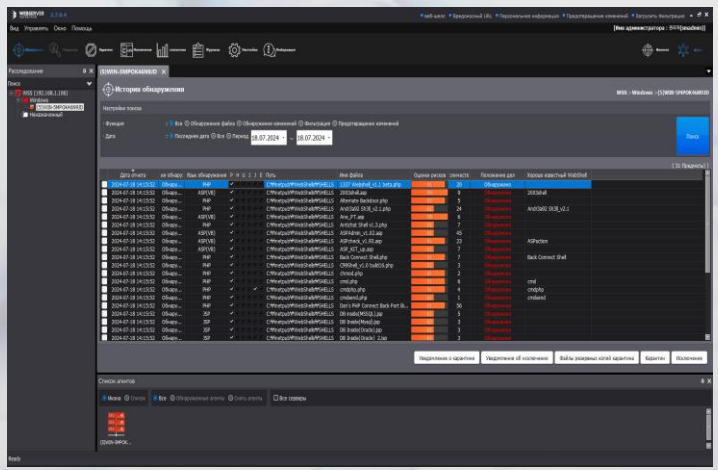
4. Основная функция WSS

Функции обнаружения веб-оболочек и вредоносных URL-адресов

Имя функции	Функциональность	Описание
Обнаружение WebShell в режиме реального времени	**Обнаружение**	Обнаружение и составление отчетов о файлах webshell с помощью полного обнаружения в режиме реального времени
	Действия по истории обнаружения	Меры против обнаружения подробностей посредством карантинных и исключительных мер.
Обнаружение вредоносных URL в режиме реального времени	**Обнаружение**	Обнаружение и сообщение о вредоносных URL-адресах с помощью полного обнаружения в режиме реального времени
	Действия по истории обнаружения	Карантин, частичный карантин и исключения для обнаруженных URL-адресов
	Функции управления	Управление URL-адресами с помощью серых, белых и черных списков.



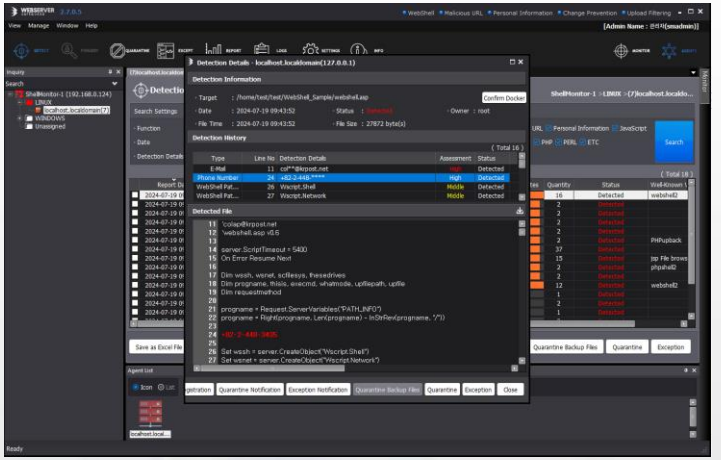
[Экран подробной информации об обнаружении]



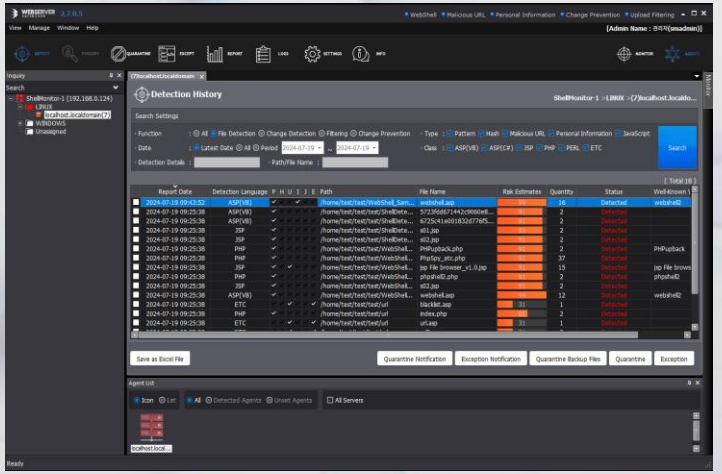
4. Основная функция WSS

Обнаружение изменения настроек окружающей среды и другие функции

Имя функции	Функциональность	Описание
Веб-сервер/WAS Конфигурация Обнаружение изменений	**Управление файлами конфигурации веб-сервера**	Сообщает администратору, если в файл конфигурации веб-сервера вносятся произвольные или злонамеренные изменения.
Обнаружение личной информации в файлах и БД	**Обнаружение личной информации (файл)**	Обнаружение и сообщение личной информации в файлах веб-сервера (PDF, HWP, DOC, PPT, EXCEL, TXT и т.д.)
	Обнаружение личной информации (БД)	Обнаружение и сообщение личной информации в БД
Фильтрация загруженных файлов	**Фильтрация файлов**	Доска объявлений для загрузки файлов. Фильтрация неавторизованных файлов.
Реакция на нарушение	**Обнаружение IP-адреса злоумышленника**	При запуске веб-оболочки проанализируйте журнал веб-сервера/WAS и сообщите IP-адрес выполнения.



[Экран обнаружения личной информации]

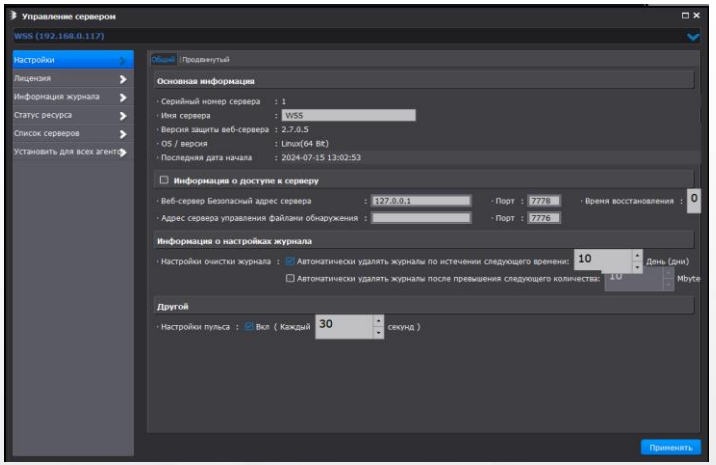


[Экран уведомления об обнаружении]

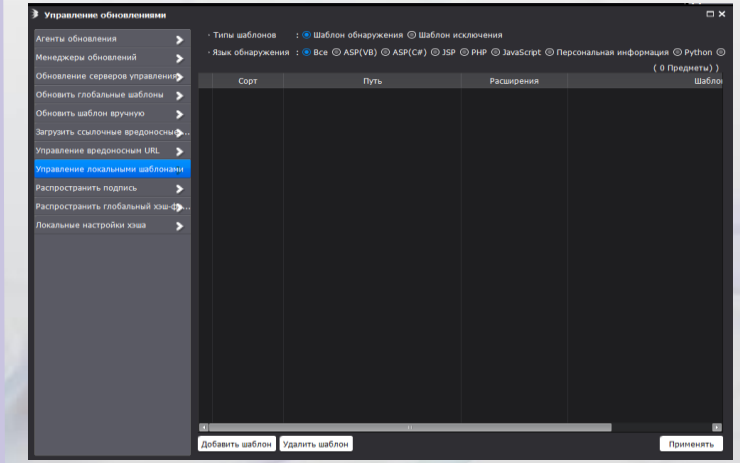
4. Основная функция WSS

Функции управления

Имя функции	Функциональность	Описание
Функция управления	**Управление обновлениями**	Агент, менеджер, обновление шаблонов и управление версиями
	Оповещение об обнаружении и интеграция с внешними системами	Обеспечивает взаимосвязь и интерфейс с внешними системами, такими как экран управления, ESM, SMS, EMAIL и т.д.
	Управление учетными записями и правами пользователей	Управление разрешениями по учетным записям и пользователям
	Статистика и отчетность	Предоставленные отчеты и статистические данные.
	Стабильность	Настройка скорости использования ресурсов установленного веб-сервера/поддержка дублирования серверов управления WAS (Active/Active)



[Экран настройки среды]



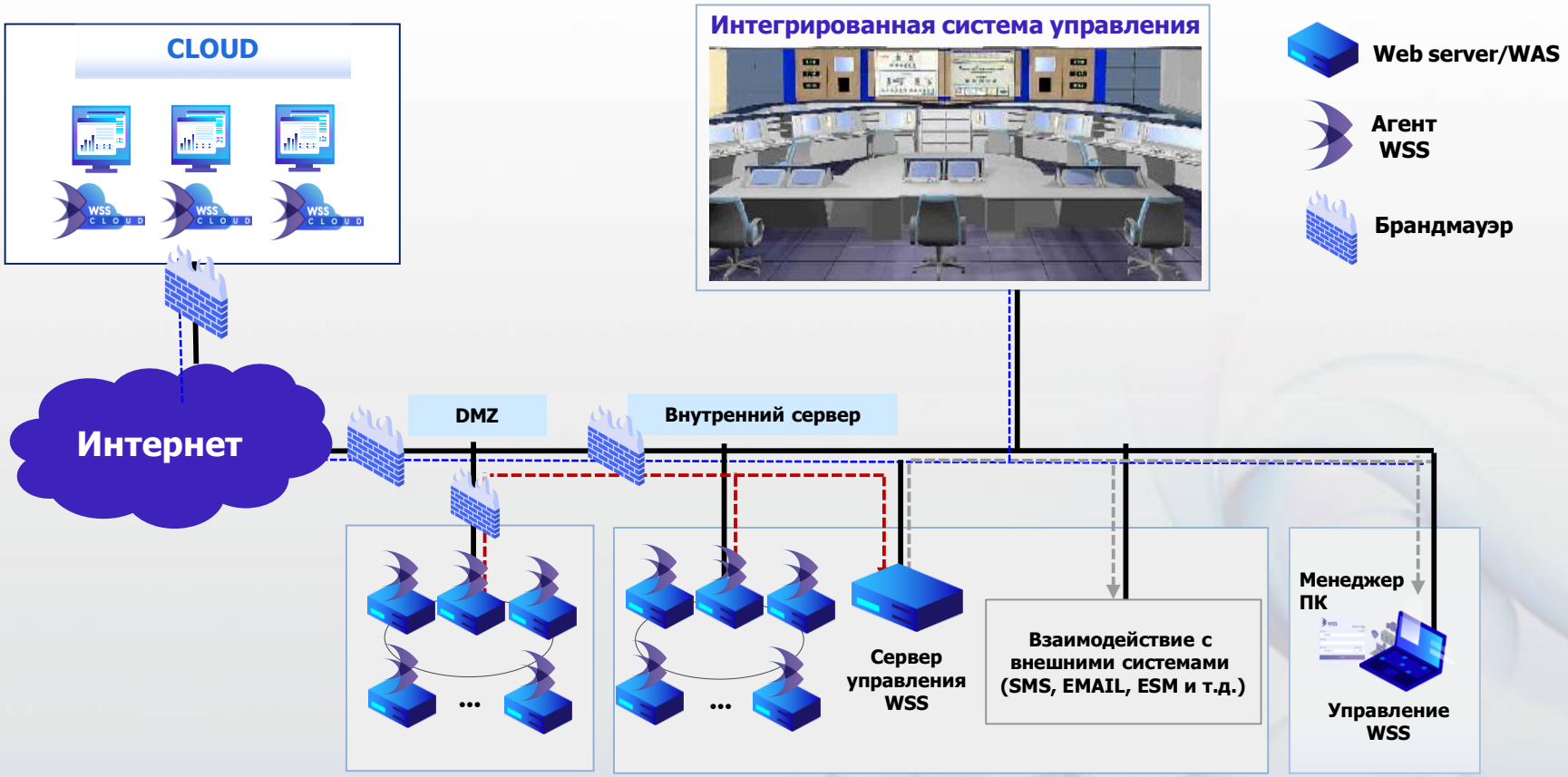
[Экран управления обновлениями]

Функции с поддержкой облачных вычислений

Имя функции	Функциональность	Описание
Поддерживает функцию Scale IN/OUT	**Scale OUT**	Автоматическое обнаружение после автоматической регистрации цели обнаружения при отключении службы WEB/WAS
	Scale IN	Автоматическое сохранение истории (журнала) обнаружения/изменения/ удаления службы WEB/WAS на сервере управления при масштабировании службы WEB/WAS.
Поддержка Docker/Container	**Предоставлена основная информация**	Предоставляет базовую информацию о Docker для функции агента.
	Классификация и обработка	Классификация контейнеров и обработка обнаруженных файлов

WSS Configuration

On-Premise /Облачные Вычисления/ Интегрированное Управление



Основные клиенты

Государственные учреждения

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

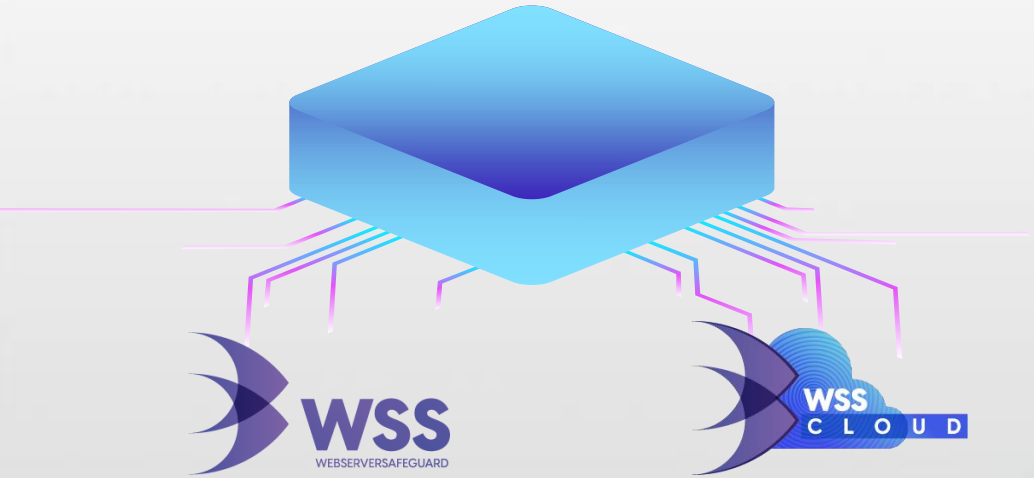
Финансы

Hana Financial Group
NH Bank
KDB Bank
Samsung Card
Hyundai Capital
Samsung Life Insurance
Samsung
BCcard
LOTTE CARD

Предприятие

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
Hanwha
S-OIL
Prudential
Pantech
GS
gabia.
SK infosec
Travel Mate

Полная безопасность веб-сервисов благодаря обнаружению и изоляции в режиме реального времени



▶ Watch Video

Спасибо.

Телефон : +77085944706
Веб-сайт: www.umvglobal.com
Email: zhuldyzay@umvglobal.com