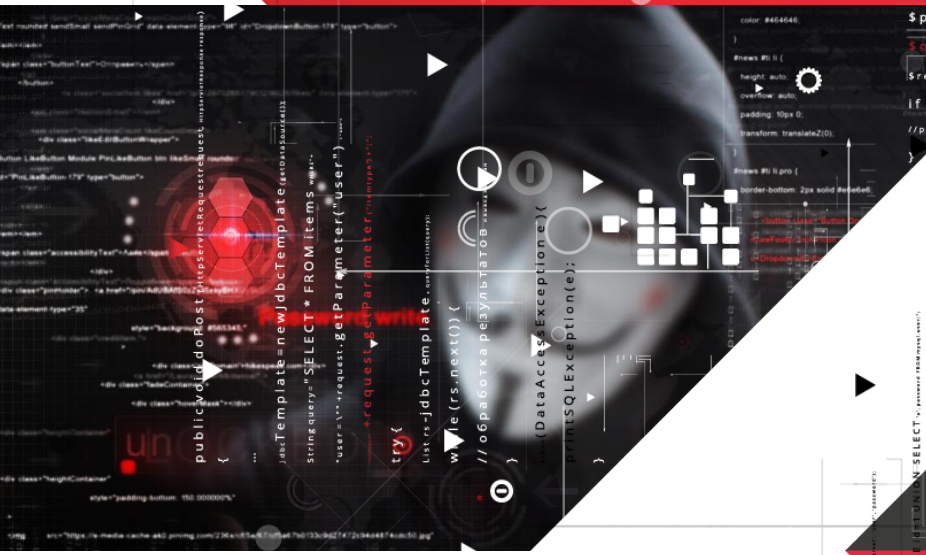
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

1 НОЯБРЯ 2018
ТЮМЕНЬ

#CODEIB

attack + killer



Прямая и неявная угроза. Инструменты защиты веб-приложений.

Воронко Алексей, зам. коммерческого директора ООО «ИнфоВотч-Урал»

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 ноября | Тюмень

Противостояние в кибер-пространстве

Атаки

Стоимость снижается (от 5$/час)

Количество растет на 50-70% в год

Комплексные атаки: DDoS + таргетированные атаки

Каждый 3й web-ресурс содержит известные уязвимости

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Техническая составляющая	Функциональные последствия	Социальные последствия
Недоступность сайта для клиентов	Невозможность получить информацию или электронную услугу	Отказ граждан от эл. госуслуг, рост нагрузки на приемные, имиджевые потери
Кража информации и ПДн	Компрометация чувствительных данных	Санкции регуляторов: штрафы, определения в адрес ответственных лиц
Подмена информации, размещение противозаконного контента	Получение неверной информации о государственном органе, его позиции, мероприятиях	Снижение уровня доверия к органу власти и государству, имиджевые потери, штрафы
Атаки на пользователей сайта	Снижение доверия, понижение позиций в поисковике	Снижение уровня доверия к органу власти и государству, имиджевые потери

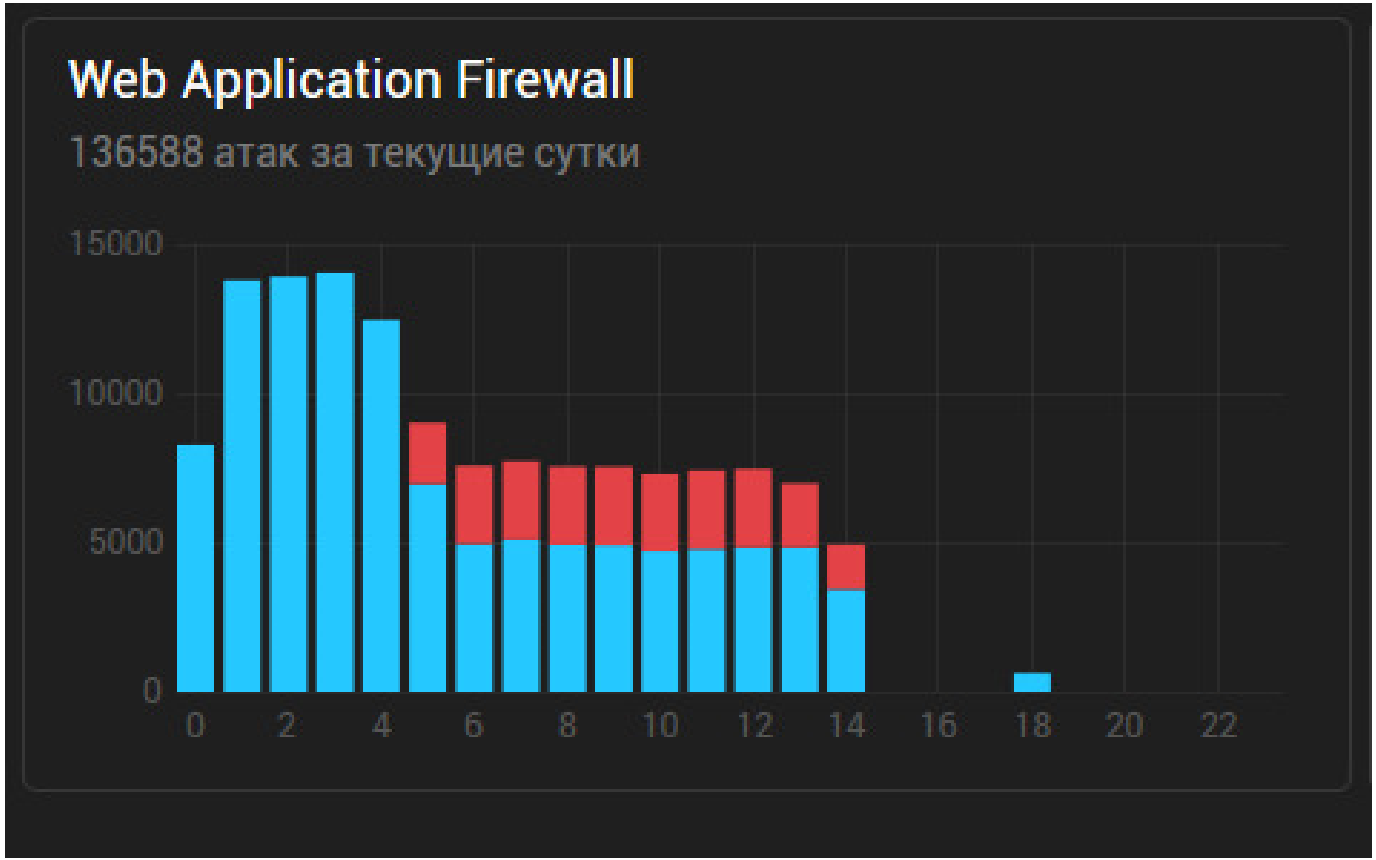
Пример успешной атаки на официальный портал муниципалитета

на официальном ресурсе муниципалитета публикуется информация о сборе гуманитарной помощи детям Донбасса

в течение часа ИТ-служба сталкивается с DDOS-атакой уровня веб-приложения

атакующая ботнет-сеть, используя «форму обращений граждан к главе города», перегружает запросами веб-сервисы и инфраструктуру, генерируя сверхвысокие нагрузки на аппаратные подсистемы. Деградируют внутренние сервисы

Официальный портал муниципалитета под защитой IW Attack Killer



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пример успешной реализации защиты с применением IW Attack Killer

www.tyumen-city.ru

под защитой IW Attack Killer

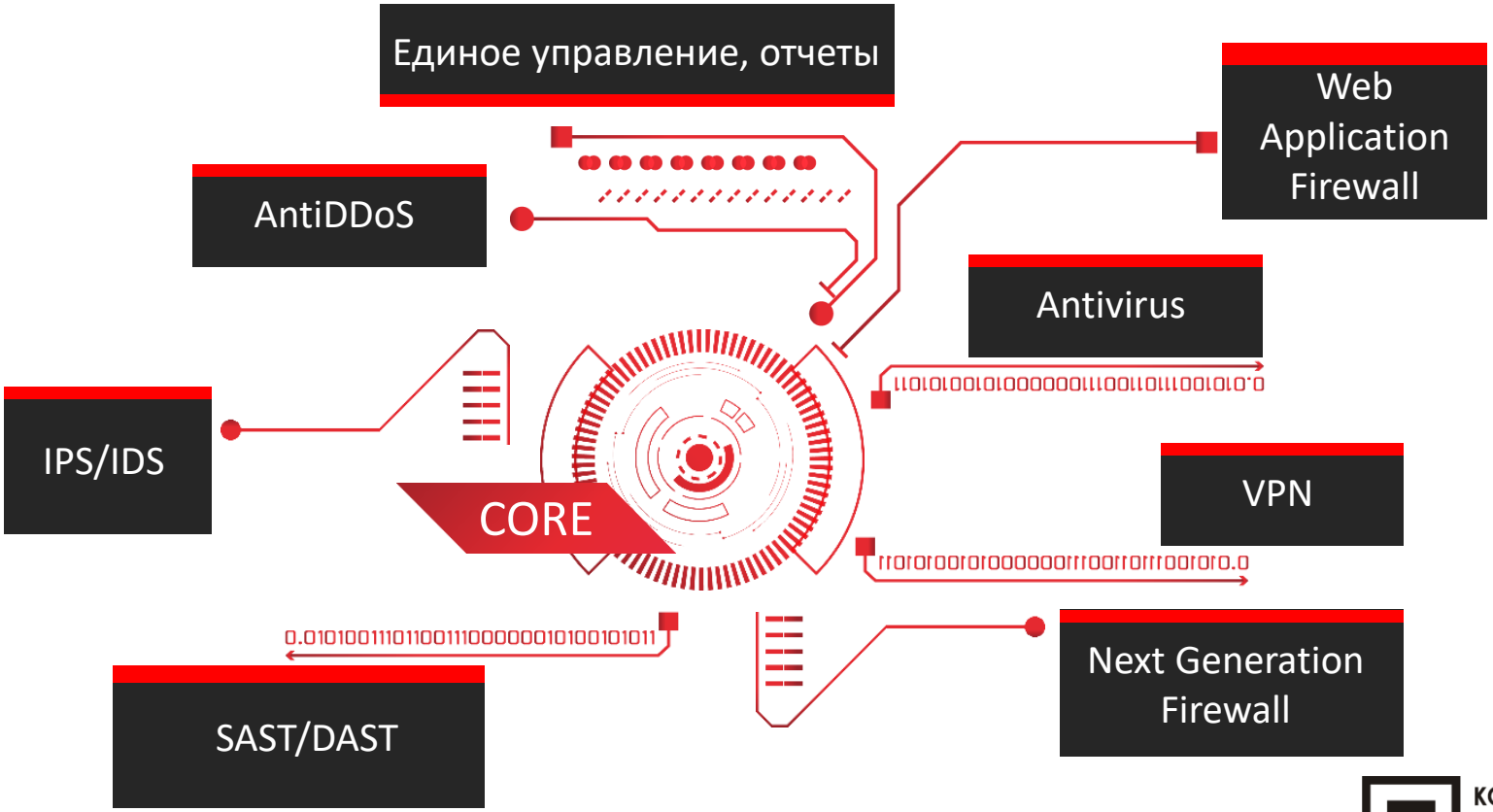
Межсетевой экран уровня веб-приложения (WAF)

Анализатор исходного кода приложений (CCS)

Единая панель управления и мониторинга

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ATTACK KILLER: наш подход к ИБ



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Attack Killer AntiDDoS: как это работает

Весь защищаемый траффик постоянно направляется через сеть фильтрующих узлов

Самообучение системы позволяет выявлять и реагировать на новые виды DDoS

«Чистый» траффик передается клиенту через Интернет, либо через специальный выделенный канал

!

AntiDDoS – это распределенная сеть фильтрующих узлов, расположенную на магистралях крупнейших Интернет-провайдеров России, США, Европы и Азии

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Attack Killer WAF: как это работает

Автоматически непрерывно изучает web-инфраструктуру (поведение пользователей & DAST)

Экспертное облако WAF анализирует полученные данные и выявляет «норму» работы

Автоматически блокирует аномальные запросы пользователей

Выпускает виртуальные патчи для закрытия обнаруженных уязвимостей web-ресурса

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Attack Killer CCS: как это работает

Анализ исходного кода WebApp на основе технологий статического анализа (SAST)

Формирует отчет об обнаруженных уязвимостях и ошибках в коде, с рекомендациями по устранению

Ставит задачу разработчикам на устранение найденных уязвимостей и багов, и проверяет выполнение задачи

Интеграция с DAST позволяет проверить найденные уязвимости на возможность взлома.
При интеграции с WAF выпускает виртуальный патч

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Attack Killer: итоги

attack + killer

Спасибо за внимание!

Алексей Воронко

Зам. коммерческого директора

ИнфоВотч-Урал

AV@infowatch.com

+7 (922) 265-26-26

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ