

КОМПЛЕКСНАЯ ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК

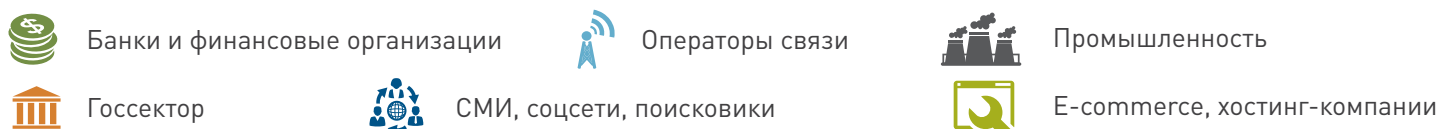
Многовекторные таргетированные или целенаправленные атаки представляют собой организованный комплекс действий злоумышленников против конкретной организации. Отдельными элементами цепи спланированных действий становятся известные угрозы: внедрение специализированного вредоносного программного обеспечения, методы социальной инженерии, эксплуатация уязвимостей веб-инфраструктуры и кода бизнес-приложений, DDoS-атаки. Чаще всего целью хакеров является воровство платежных данных и коммерческих секретов, хищение средств, а также вывод из строя критически важных объектов инфраструктуры.



УЩЕРБ ДЛЯ БИЗНЕСА ОТ МНОГОВЕКТОРНЫХ ТАРГЕТИРОВАННЫХ АТАК

- Вывод из строя объектов, критически важных для бизнеса
- Прямой финансовый ущерб из-за дестабилизации работы веб-ресурсов
- Репутационные потери
- Утечка платежных данных, конфиденциальной информации, ноу-хау, коммерческой тайны
- Перенаправление счетов, воровство и мошенничество
- Кража и продажа персональных и финансовых данных

ОТРАСЛИ ПОД ПРИЦЕЛОМ



Бурный рост таргетированных атак

За 2014г. количество таргетированных атак увеличилось на 48% по сравнению с 2013г. При этом 66% инцидентов безопасности остаются незамеченными месяцами.

DDoS становится популярней

Рост числа DDoS-атак в мире составляет 18-20%, в России эта цифра приближается к 25% в год.

Большинство веб-приложений имеют критические уязвимости

При первом аудите практически каждое веб-приложение содержит около 5 уязвимостей, которые могут быть использованы злоумышленниками.

ПРИВЫЧНЫЕ УГРОЗЫ – НОВЫЙ ПОДХОД

Эксплуатация уязвимостей приложений и DDoS-атаки позволяют хакерам не только получить контроль над ресурсом, но и проникнуть во внутреннюю инфраструктуру компании. Внедренное вредоносное ПО способно месяцами оставаться незамеченным и наносить ущерб организации. **Хакеры используют комплексный подход к реализации атаки, поэтому базовые средства безопасности не способны обеспечить эффективную защиту.**

МНОГОВЕКТОРНАЯ ТАРГЕТИРОВАННАЯ АТАКА ЭТО

- Спланированная
 - Многоступенчатая
 - С четкой целью
 - Высокой сложности
 - С использованием специальных методов обхода защиты
 - Направленная на конкретную организацию
- Это не просто «зловредное» ПО**
- комплексная атака**

*По данным аналитического центра InfoWatch, Neustar и других агентств

*** По данным Group-IB

**Сайт Sony Pictures взломан, украдены данные 1 миллиона аккаунтов, Habrahabr.ru

**** Ущерб от уязвимости Heartbleed оценивается в \$500 млн, Хакер.ru

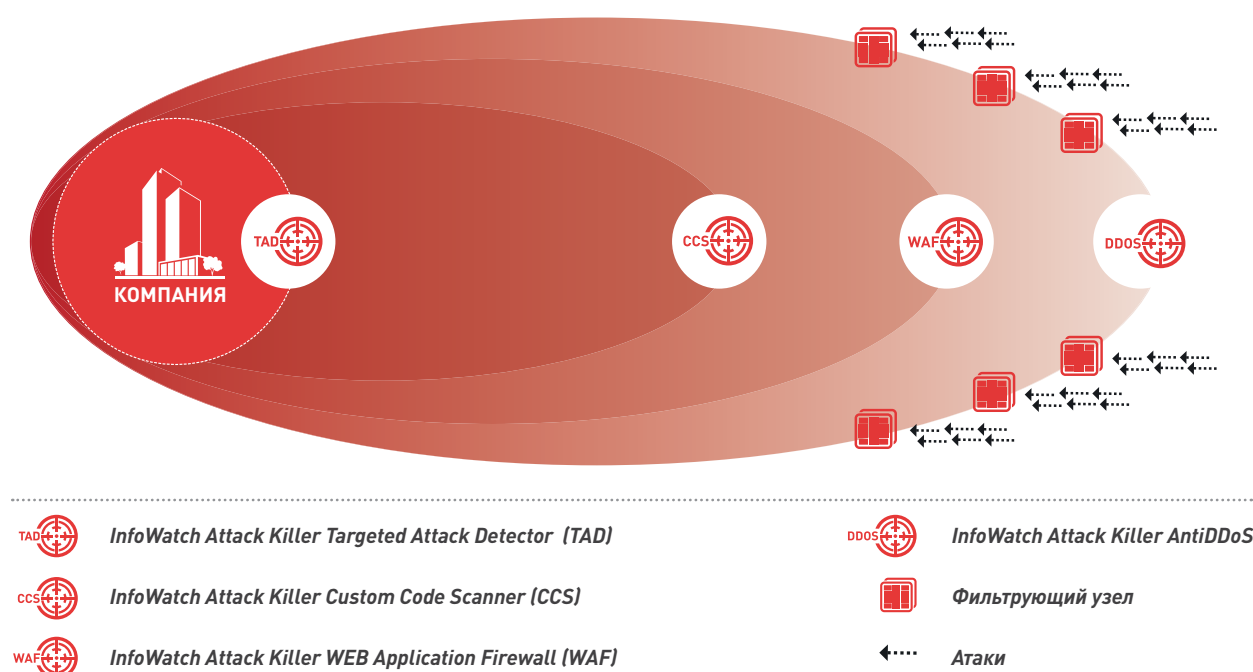
СЦЕНАРИЙ РЕАЛИЗАЦИИ МНГОВЕКТОРНОЙ ТАРГЕТИРОВАННОЙ АТАКИ

Разведка ➡➡ Отвлечение внимания ➡➡ Вход в систему ➡➡
➡➡ Ожидание удобного момента ➡➡ Атака ➡➡ Соккрытие следов

*Противостоять таким
атакам может лишь
автоматизированное
самообучающееся
комплексное решение класса
Continuous Security*

МНОГОУРОВНЕВАЯ ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК

Комплексный подход InfoWatch и непрерывность процесса позволяет защитить ресурсы компании как на уровне операционной системы и серверов, так и на уровне веб-инфраструктуры, которая чаще всего становится для злоумышленников точкой проникновения.



Модуль **InfoWatch Attack Killer Targeted Attack Detector (TAD)** предназначен для обнаружения таргетированных атак внутри компании. Самообучающаяся экспертная облачная система проводит непрерывный мониторинг ИТ-инфраструктуры и анализирует полученные данные на наличие в ней аномальных активностей. Использование нескольких видов анализа обеспечивает высокую точность классификации аномалий. Решение поможет выявить вредоносное ПО, которое было внедрено в компанию до начала эксплуатации решения TAD.

Модуль **InfoWatch Attack Killer AntiDDoS** работает на внешнем периметре сети и в непрерывном режиме защищает организацию от DDoS-атак. Распределенная сеть фильтрующих узлов, расположенная на магистральных крупнейших интернет-провайдеров, гарантирует блокировку DDOS-атак на начальном этапе.

Модуль **InfoWatch Attack Killer WEB Application Firewall (WAF)** работает на уровне защиты веб-инфраструктуры. Благодаря самообучающимся алгоритмам система обеспечивает эффективную защиту от различных хакерских атак в автоматическом режиме. При совместном использовании модулей WAF и AntiDDoS клиент получает возможность блокировать попытки эксплуатации уязвимостей на уровне сети фильтрующих узлов, тем самым снижая нагрузку на приложение.

Модуль **InfoWatch Attack Killer Custom Code Scanner (CCS)** детектирует уязвимости кода приложений и передает собранную информацию на модуль WAF для принятия мер по их закрытию. Интеграция модулей CCS и WAF позволяет выявить из множества событий безопасности векторы атак, которые могут стать реальными инцидентами. Обнаруженные методами статического и динамического анализа критические уязвимости автоматически закрываются виртуальными патчами.

Конфигурация и управление всеми компонентами InfoWatch Attack Killer осуществляется через удобный единый веб-интерфейс. Клиент всегда может проверить состояние системы, получить детализированные отчеты о всех выявленных проблемах и угрозах. Для интерпретации отчетов не требуется специализированных знаний благодаря наглядной визуализации атак и подробным экспертным рекомендациям по устранению проблем.

InfoWatch Attack Killer уникальный продукт, не имеющий аналогов в мире. Обеспечивает комплексную защиту от многовекторных таргетированных атак и включает в себя **4 модуля**:



InfoWatch Attack Killer Targeted Attack Detector (TAD) – модуль обнаружения вредоносного программного обеспечения на рабочих станциях и серверах посредством статического и динамического анализа аномалий.

- С помощью анализа аномалий выявляет таргетированные атаки, реализуемые злоумышленниками с использованием специализированного программного обеспечения
- Осуществляет непрерывный мониторинг изменений состояния ИТ-системы и позволяет обнаружить замысел противника
- Благодаря самообучающимся алгоритмам экспертная облачная система с высокой точностью классифицирует обнаруженные аномалии
 - при необходимости к анализу подключаются аналитики InfoWatch



InfoWatch Attack Killer Custom Code Scanner (CCS) – модуль выявления уязвимостей в коде веб-приложений.

- Обнаруживает ошибки в исходном коде с учетом требований по безопасному программированию PCI DSS, OWASP, рекомендаций SDLC, а также производителей платформ
- Поддерживает все самые известные языки программирования (Java, PHP, JavaScript, C# и др.)



InfoWatch Attack Killer WEB Application Firewall (WAF) – модуль для предотвращения хакерских атак на веб-приложения и обнаружения уязвимостей веб-инфраструктуры.

- Автоматически непрерывно изучает веб-инфраструктуру компании
 - отправляет на анализ в облачную экспертную систему поведенческую статистику пользователей, результаты динамического сканирования ресурсов
 - на основе информации об уязвимостях, найденных модулем CCS, WAF выявляет какие из них могут стать реальными инцидентами ИБ
- Экспертная система WAF на основе всей собранной информации определяет «норму» работы веб-инфраструктуры и блокирует все аномальные действия (отличные от нормы)
 - выпускает виртуальные патчи для блокировки аномальных запросов до исправления уязвимостей разработчиками
 - анализируя аномалии в неструктурированных событиях находит логику и объединяет их в инцидент, определяя вектор атаки



InfoWatch Attack Killer AntiDDoS – модуль позволяет выявлять и гарантированно предотвратить масштабные DDoS-атаки.

- Блокирует масштабные DDoS-атаки на начальном этапе благодаря распределенной системе узлов фильтрации
 - отказ любого из узлов не вызовет изменений в качестве обслуживания (BGP Anycast)
- Защищает ресурс непрерывно и в автоматическом режиме сразу после подключения
 - в случае атаки от клиента не потребуются дополнительных действий
- Обеспечивает защиту для большинства протоколов (HTTP, HTTPS, DNS, SIP и др.)

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

• **Единственное в мире решение**, реализующее многоуровневый подход к обнаружению и защите от большинства таргетированных атак

• **Союз лучших в своем классе**

Комплексное решение представляет синергию 4 технологий, лидирующих в своих продуктовых нишах

• **Удобное управление через единый веб-интерфейс**

Решение управляется из единой консоли и создает детализированные отчеты о зафиксированных таргетированных атаках, найденных уязвимостях и попытках их эксплуатации, аномальной активности приложений и DDoS-атаках

• **Помогает выполнять требования регуляторов**

Приказ ФСТЭК России №21 и №17, ФЗ-№152, PCI DSS, СТО БР, НДБ4, SDL

• **Простое автоматизированное решение**

Не требует дополнительных ресурсов на обслуживание и поддержку

• **Решение-конструктор**

Позволяет использовать каждый модуль по отдельности, в любых сочетаниях, а также быстро расширить используемый комплекс до полного комплекта

ЗАЩИТУ ИСПОЛЬЗУЮТ

ANTIDDOS POWERED BY QRATOR



Тинькофф
Кредитные Системы

ЭЛЬДОРАДО

WAF POWERED BY WALLARM



ЮЛМАРТ
КИБЕРМАРКЕТ

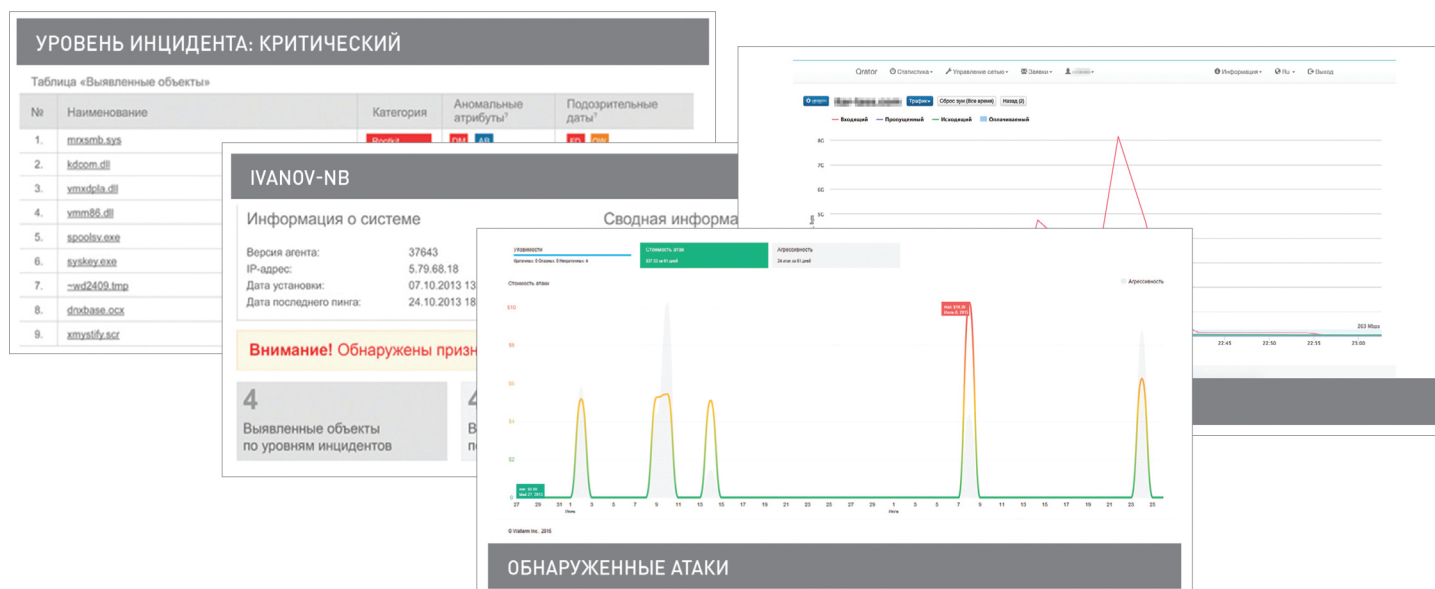


QIWI
КИВИ

CCS POWERED BY APPERCUT



ГАЗПРОМБАНК



О ГК INFOWATCH

Группа компаний InfoWatch объединяет ряд российских и зарубежных разработчиков программных продуктов и решений для обеспечения информационной безопасности организаций, противодействия внешним и внутренним угрозам. InfoWatch обладает обширной экспертизой и опытом реализации проектов информационной безопасности любой сложности в государственном секторе, ТЭК, финансовой, телекоммуникационной и многих других отраслях экономики.

МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ.