INFOWATCH TARGETED ATTACK DETECTOR

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ЗАЩИТА ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК

ТЕНДЕНЦИИ

За последние несколько лет крупные компании все чаще и чаще стали подвергаться целенаправленным хакерским атакам. Данные инциденты не проходят незамеченными и приводят к серьезным последствиям, в том числе и финансовым.

Постоянно растущий уровень конкуренции толкает организации на радикальные меры по «уничтожению» своих оппонентов.

Целенаправленные атаки – один из изощренных способов ведения конкурентных войн при помощи хакерских атак. Компании стремятся выведать коммерческие секреты и нанести финансовый ущерб своим конкурентам. Хакеры пытаются заработать на перепродаже полученных сведений, краже денежных средств и коммерческой тайны, уничтожении ИТ-инфраструктуры, компрометации ключевых персон.

РОСТ ЧИСЛА ЦЕЛЕНАПРАВЛЕННЫХ АТАК

2013	29 млн инцидентов	
2014	42,8 млн инцидентов	**+ 48%**

В среднем каждый день совершалось **117 260** кибератак.

Размер убытка от утраты информации, составляющей коммерческую тайну, может находиться в диапазоне от **749** миллиардов до **2,2** триллиона долларов США в год.

**По данным PWC*

63% компаний уверены, что целенаправленная атака на их организацию — вопрос времени

67% опрошенных компаний признают, что принятые у них меры безопасности не в состоянии защитить их от направленной атаки

**По данным опроса ISACA*

НЕМНОГО КОНКРЕТИКИ

Атака Carbanak

Злоумышленники проводили адресные рассылки электронных писем, содержащих вредоносные вложения, сотрудникам атакуемых финансовых учреждений. Через полученные уязвимости хакеры получали доступ к интересующим их объектам сети банка. Убытки каждого из банков составляют от 2,5 до 10 млн долларов США, а суммарные убытки банков, зараженных Carbanak, достигают миллиарда долларов США.

Атака на Boleto

В 2014 году атаке подверглась бразильская платежная система Boleto. Всего в Бразилии было обнаружено 192 227 жертв взлома Boleto, которые были клиентами 34 банков. Злоумышленникам удалось перехватить 495 793 транзакций через Boleto, что повлекло за собой ущерб в размере 3,5 млрд долларов США.

Атака на Orange

Французский телекоммуникационный оператор Orange сообщил о хакерской атаке на свою инфраструктуру,

в результате которой были скомпрометированы 800 тыс. записей клиентов компании. Доступ к персональным данным — именам, номерам телефонов, адресам электронной почты и пр. — хакеры получили путем взлома клиентской части официального сайта компании.

Атака на Home Depot

Крупнейшая в мире компания по продаже стройматериалов и ремонтных приспособлений Home Depot заявила, что 53 млн адресов электронной почты клиентов сети магазинов были скомпрометированы. По предварительным подсчетам, убытки Home Depot вследствие взлома составили 56 млн долларов США.

КТО БОЛЕЕ ПОДВЕРЖЕН РИСКУ

15%	Промышленность и транспорт
30%	Банки и Финансы
17%	Наукоемкие производства
11%	Телекоммуникационные компаниии
20%	Нефтегазовая индустрия
7%	Другие

**По данным опроса ISACA*

INFOWATCH TARGETED ATTACK DETECTOR

ОТЛИЧИЕ МАССОВЫХ И ЦЕЛЕНАПРАВЛЕННЫХ АТАК

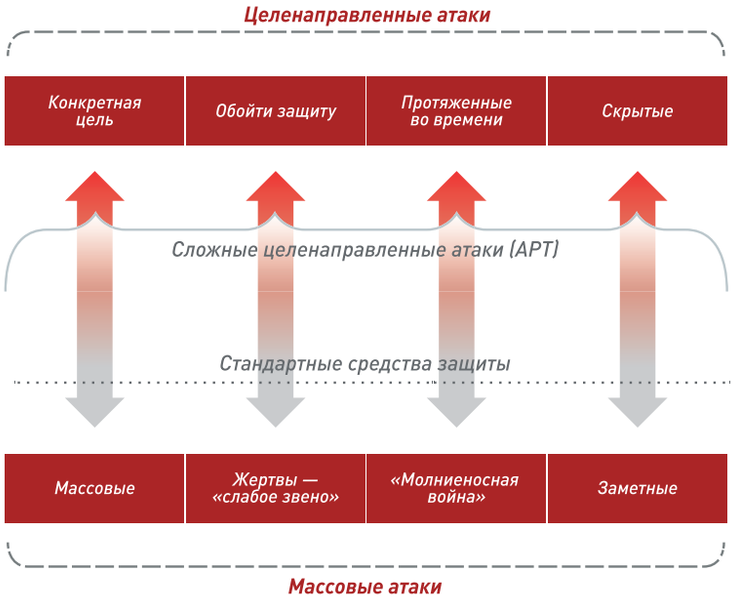
Конкретная жертва. Атакующего интересует заранее определенная компания или государственная организация. С помощью атаки решаются конкретные задачи, связанные с получением выгоды.

Первостепенная задача – обойти защиту. Атакуемый объект всегда защищен. Для успеха атаки защиту нужно уметь обходить или отключать. Злоумышленники используют уникальные вредоносные программы, уязвимости (0day) и социальную инженерию.

Адаптивность и протяженность во времени. Атакующая сторона постоянно адаптирует методы атаки. Неудачная попытка не может остановить злоумышленников – они придумают более изощренный метод и повторят атаку.

Компрометация ключевых лиц. Получив необходимые сведения в результате атаки на ИТ-инфраструктуру, злоумышленники могут шантажировать компании или перепродать сведения для получения материальной выгоды.

ОСНОВНОЙ УЩЕРБ ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК – ПРЯМЫЕ ДЕНЕЖНЫЕ ПОТЕРИ, ВОРОВСТВО СЕКРЕТНОЙ ИНФОРМАЦИИ, СНИЖЕНИЕ КОНКУРЕНТОСПОСОБНОСТИ И РЕПУТАЦИОННЫЕ РИСКИ



Наличие заказа. Данный тип атаки имеет заказной характер, поэтому вредоносная программа всегда уникальна.

Скрытность. Задача злоумышленников – закрепиться в атакуемых системах и как можно дольше оставаться незамеченными, поскольку это позволяет постоянно похищать конфиденциальную информацию. Почти во всех получивших известность целенаправленных атаках использовались вредоносные программы, которые оставались неизвестными на протяжении нескольких лет.

КАКИЕ ДАННЫЕ ЧАЩЕ ВСЕГО ПОХИЩАЮТ?

37%	23%	19%	13%	8%
Платежная информация	Персональные данные, клиентские базы	Коммерческая тайна, know-how	Конфиденциальная информация	Государственная тайна

**По данным опроса ISACA*

НЕОБХОДИМОСТЬ НОВЫХ МЕТОДОВ ЗАЩИТЫ

ЗА ПОСЛЕДНИЕ ГОДЫ УГРОЗЫ СУЩЕСТВЕННО ИЗМЕНИЛИСЬ – ОНИ ЭВОЛЮЦИОНИРОВАЛИ

Целенаправленные атаки имеют ряд особенностей, которые не позволяют использовать для защиты от них традиционные методы безопасности. Среди таких особенностей: использование уникальных инструментов атак, профессиональный подход к разработке атак, поэтапность атак и протяженность во времени, скрытность. Стандартные методы обнаружения атак оказываются неэффективными, что в большинстве случаев приводит к повышению финансовых и репутационных рисков, снижению конкурентоспособности и прямым финансовым потерям.

СТАНДАРТНЫЙ ПОДХОД ОБНАРУЖЕНИЯ АТАК

- **Поиск последствий**
- **Поиск вредоносного кода**

Накопив достаточно опыта и знаний, злоумышленники получили возможность изучать методы защиты и обходить стандартные средства обеспечения безопасности, поэтому стандартные средства защиты оказываются бессильны при целенаправленных атаках. При целенаправленных атаках ИТ-инфраструктура компании подвержена большому риску, что может привести к потере денежных средств и прерыванию бизнес-процесса.

INFOWATCH TARGETED ATTACK DETECTOR

ПОДХОД INFOWATCH

АРХИТЕКТУРА

Агент

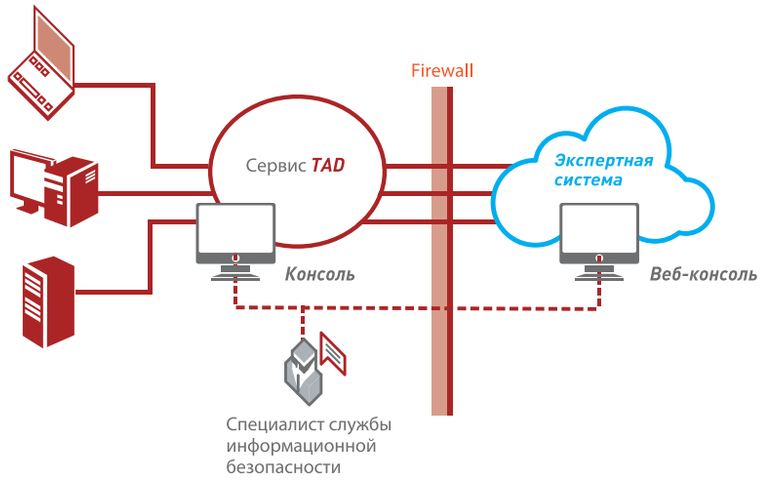
На каждый компьютер компании устанавливается агент, выполняющий непрерывный мониторинг ИТ-инфраструктуры.

Сервер

Позволяет осуществлять централизованную установку агентов и контроль данных, передающихся в облачную систему.

Экспертная система

Уникальная облачная система, выявляющая аномалии и классифицирующая большие массивы данных (Big Data).

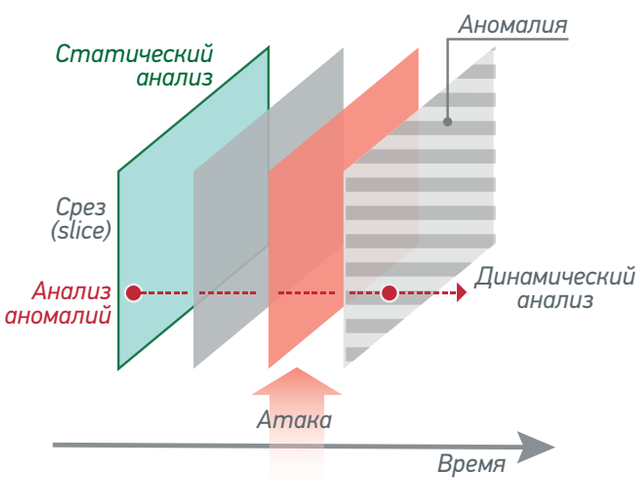


Личный кабинет

Позволяет получить наглядные отчеты о текущем состоянии агентов, а также статистику по всем инцидентам.

КАК ЭТО РАБОТАЕТ?

Продукт InfoWatch Targeted Attack Detector основан на контекстном анализе изменений операционной системы, выявлении и анализе аномалий во времени. Решение постоянно выполняет сканирование с целью сбора и классификации широкого спектра характеристик объектов системы. Результатом сканирования является срез системы (slice), который подвергается нескольким видам анализа.



ТЕХНОЛОГИИ АНАЛИЗА

1. Статический анализ

Цель – классификация всех объектов, входящих в срез системы (slice).

2. Динамический анализ

Цель – изучение аномалий во времени и их классификация.

3. Анализ аномалий

Цель – классификация аномалий и определение точного вердикта.

ПОДХОД INFOWATCH TARGETED ATTACK DETECTOR

- **Непрерывный мониторинг ИТ-инфраструктуры**
- **Статический и динамический анализ**

Уникальные технологии платформы InfoWatch Targeted Attack Detector позволяют проводить анализ на основе собранного контента, точно выявляя аномальные изменения. Решение осуществляет все операции с высокой скоростью и максимально точно классифицирует выявленные аномалии, за счет самообучающейся экспертной системы и привлечения аналитиков компании InfoWatch.

СЕРВЕР ЦЕНТРАЛИЗОВАННОЙ УСТАНОВКИ АГЕНТОВ ПОЗВОЛЯЕТ:

- производить удобную централизованную установку, обновление и удаление агентов продукта без использования стандартных средств установки
- получать информацию о текущем состоянии агентов
- контролировать отправляемые в облако файлы (с автоматическим временем отправки без участия пользователя)
- объединить все агенты продукта в закрытую локальную сеть, где выход в Интернет имеет только один централизованный сервер

INFOWATCH TARGETED ATTACK DETECTOR

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ПРЕИМУЩЕСТВА

Эффективная защита ценной информации, снижение репутационных и финансовых рисков

InfoWatch Targeted Attack Detector выявляет целенаправленную атаку и избавляет компании и организации от финансовых и репутационных рисков, которые могут быть связаны с компрометацией информационных систем и кражей конфиденциальной информации и персональных данных.

Уникальные технологии по обнаружению специализированного ПО

Изучение тактики и методов, которые используют злоумышленники при создании вредоносного ПО для целенаправленных атак, позволили компании разработать уникальные технологии защиты. Решение выявляет такие атаки, где используются еще неизвестные (0day) уязвимости и вредоносные программы, применяются новые методы внедрения и закрепления ПО в ИТ-систему.

Быстрая и точная классификация аномалий

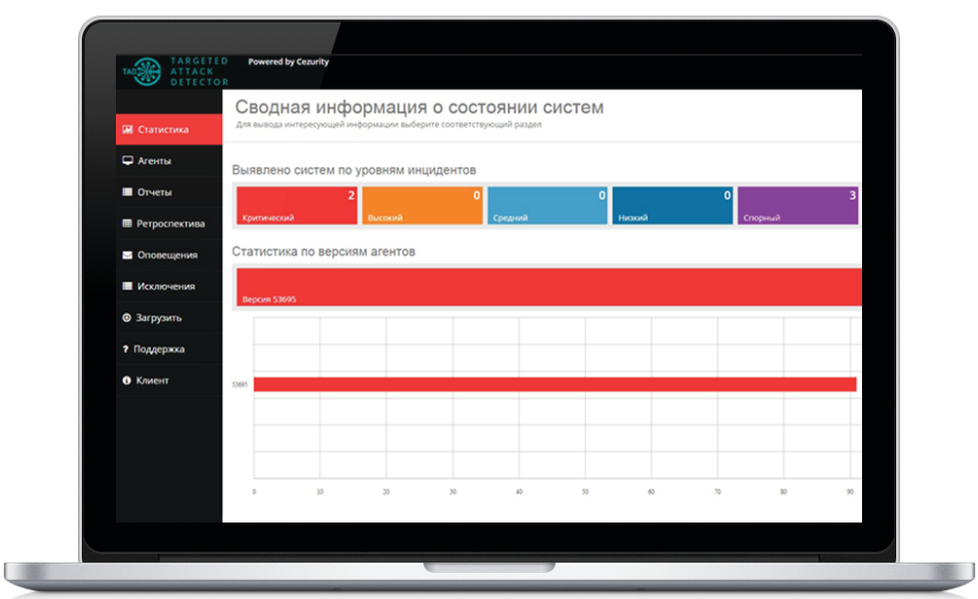
InfoWatch Targeted Attack Detector обладает обширными возможностями по выявлению аномалий. Статический и динамический анализ позволяет определить и выявить аномалию, а также точно классифицировать ее.

Простота внедрения и использования

Решение не зависит от инфраструктуры и топологии защищаемой информационной системы. Агент InfoWatch Targeted Attack Detector устанавливается на все имеющиеся компьютеры в ИТ-инфраструктуре компании. Программное обеспечение не нуждается в обновлениях, т.к. его работа ограничивается сбором и отправкой информации в Автоматизированную Экспертную Систему. Работа решения незаметна для пользователя, так как не сказывается на производительности других приложений.
За счет того, что наиболее ресурсоемкие процессы анализа происходят в Автоматизированной Экспертной Системе (в облаке), InfoWatch Targeted Attack Detector не требует дозакупок дополнительного ПО или оборудования.

Привлечение аналитиков

Компания InfoWatch предоставляет клиентам возможность пользоваться услугами опытных аналитиков, которые с легкостью решат задачи любой сложности. Наши аналитики обладают огромным опытом по выявлению аномалий и способам борьбы с ними.



INFOWATCH® +7 (495) 22-900-22 sales@infowatch.ru www.infowatch.ru