UserGate

Решения UserGate

ДЛЯ ЗАЩИТЫ БИЗНЕСА ОТ КИБЕРУГРОЗ

UserGate SUMMA

СЛАГАЕМЫЕ БЕЗОПАСНОСТИ

Экосистема решений для комплексного подхода к обеспечению информационной безопасности

КИБЕРБЕЗОПАСНОСТЬ
для надежности бизнес-процессов

Современные кибератаки представляют собой цепочки действий, которые, на первый взгляд, могут быть не связаны друг с другом.

Главная задача злоумышленника – совершить эти действия в обход средств сетевой безопасности.

Как правило, действия злоумышленников представляют собой набор событий в корпоративной сети и запускаемые процессы на конечной станции – устройстве сотрудника.

Вас атакуют?

Может показаться, что по отдельности эти события не представляют прямой угрозы для бизнеса. Однако последовательность таких процессов сама по себе уже является киберинцидентом.

Именно поэтому одна из приоритетных задач отдела информационной безопасности – обнаружить эту цепочку действий, предотвратить ее реализацию и обеспечить непрерывность бизнес-процессов.

РИСКИ И КИБЕРУГРОЗЫ
для бизнес-процессов

Компрометация обслуживающей инфраструктуры → доступ к критической информации

Серверы, базы данных, вспомогательные системы и инструменты могут быть атакованы как снаружи, так и изнутри организации. Такие атаки позволяют злоумышленникам закрепляться во внутренней сети для реализации своих задач: организации скрытого канала управления, шпионажа, кражи персональных и коммерческих данных, кражи денежных средств.

Большинство механизмов давно известны, их можно обнаружить сигнатурным анализом сетевого трафика. Главная проблема – защищенные SSL-соединения, на которых в настоящее время работает 95% интернета.

В этих условиях основным требованием к современным средствам защиты сетевых ресурсов становится умение расшифровывать защищенный трафик и проверять его содержимое на предмет вредоносного кода.

Выведение из строя обслуживающей инфраструктуры → остановка бизнес-процессов

Любое IT-окружение, участвующее в бизнес-процессах, имеет уязвимости, что позволяет злоумышленникам нарушать или останавливать ведение бизнеса на неопределенный срок.

Типичные примеры такого вторжения – DoS-атаки: сайт компании становится недоступен, и клиенты не могут воспользоваться им. Или атаки шифровальщиков: пользователи теряют доступ к информационным системам и рабочим файлам.

Заражение рабочих станций сотрудников → вход в сеть для злоумышленников

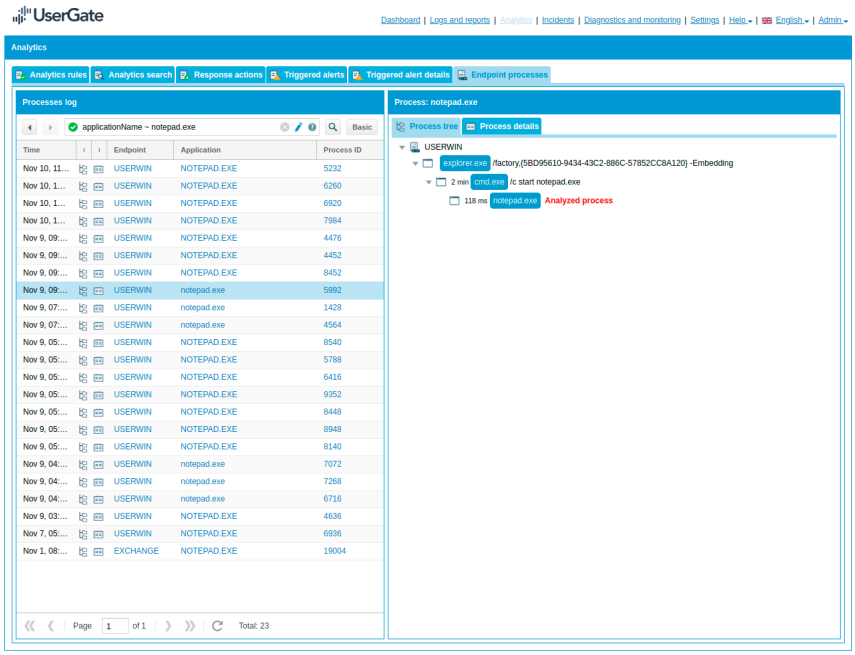
Проникновение вредоносного ПО на конечные станции сотрудников открывает злоумышленникам прямую дорогу к сетевым ресурсам организации. Очень важно не только обнаружить наличие зловреда на устройстве, но и отследить возможную цепочку атаки.

ИНСТРУМЕНТЫ UserGate SUMMA*
для обнаружения и предотвращения кибератак

Модуль СОВ (система обнаружения и предотвращения вторжений) расшифровывает все защищенные SSL-соединения и проверяет их на предмет легитимности и отсутствия вредоносного кода внутри. Использование данного модуля существенно снижает риски эксплуатации уязвимостей обслуживающей инфраструктуры, так как благодаря механизмам и технологиям предотвращается их эксплуатация.

UserGate Client отслеживает состояние рабочих станций сотрудников. Это позволяет специалисту по информационной безопасности собирать данные для последующего анализа и выявления потенциально подозрительной активности.

В UserGate Client можно увидеть цепочку запуска процессов:



Часто злоумышленники пользуются уязвимостями популярных программных продуктов (например Microsoft Excel) для запуска произвольного кода.

Таким образом, в цепочке запущенных процессов будет видно, что вместе с Excel запускался исполняемый скрипт.

UserGate Log Analyzer собирает все данные для корреляции событий и поиска инцидентов безопасности. Основными источниками для анализа могут быть UserGate Client и модуль СОВ, которые передадут информацию как с уровня сети, так и с уровня конечных станций.

Таким образом, специалист по информационной безопасности увидит всю цепочку событий, сможет предотвратить инцидент и провести расследование.

Постоянный анализ трафика, использование современных средств обеспечения информационной безопасности и регулярные обновления защитят ваш бизнес от простоя и потери чувствительной информации.

В арсенале UserGate есть все необходимые инструменты для защиты организаций любого масштаба от актуальных киберугроз.

DEMO

Вы можете оформить пробный период или запросить демонстрацию решений UserGate, направив запрос на почту sales@usergate.ru или по телефону 8 (800) 500 4032.

*__UserGate SUMMA__ – экосистема продуктов кибербезопасности, которая позволяет реализовать базовые механизмы сетевой защиты.

UserGate

Контактная информация:

Телефон: 8 (800) 500 4032
Клиентам: sales@usergate.ru
Партнерам: partner@usergate.ru
usergate.ru