Как Varonis помог крупной сервисной компании избавиться от массового заражения вредоносным ПО

ИСТОРИЯ УСПЕХА

> Что касается решений, Varonis Edge стал для нас самым ценным продуктом. Edge направляет нас к компьютерам с подозрительными DNS-запросами, сопоставляя их с конкретными пользователями и показывая нам адреса, которые нужно заблокировать.

В ЭТОЙ ИСТОРИИ

Наш клиент — крупная сервисная компания. По его просьбе мы сохраняем в тайне всю конфиденциальную информацию, включая имена отдельных лиц, название компании и отрасль.

КЛЮЧЕВЫЕ СВЕДЕНИЯ

ЗАДАЧИ

- Разобраться, почему работа сети замедлилась
- Понять масштаб заражения вредоносным ПО
- Устранить вредоносное ПО, которое заразило почти все серверы и рабочие станции

РЕШЕНИЕ

Платформа кибербезопасности Varonis в составе следующих модулей:

- **DatAdvantage** для Active Directory и Azure
- **DatAlert** для обнаружения и предотвращения угроз
- **Edge** для защиты от угроз по периметру сети, включая вредоносное ПО

ПОЛУЧЕННЫЕ РЕЗУЛЬТАТЫ

- Заражение вредоносным ПО успешно устранено
- Внедрение непрерывного мониторинга и контроль для предотвращения будущих атак

Задачи

ОБНАРУЖЕНИЕ И БЛОКИРОВКА УГРОЗЫ КРИПТОМАЙНИНГА

Признаки атаки были незаметными: компьютеры работали немного медленнее, приложения работали нестабильно, а производительность сети в целом снижалась.

Но этого было достаточно, чтобы специалисты по информационной безопасности крупной сервисной компании (пожелавшие остаться неназванными) поняли, что что-то не так.

Они решили установить Varonis DatAlert и Edge, чтобы разобраться в проблеме.

> “Мы видели, что у нас проблема, но без Varonis мы бы так и не узнали, насколько она разрушительна.”

С помощью Varonis было обнаружено, что почти все серверы и рабочие станции были заражены вредоносным ПО для майнинга криптовалют.

> “Решения Varonis помогли нам разобраться в ситуации и выявить истинную причину проблем.”

Вместо того чтобы строить майнинговые установки и самостоятельно оплачивать счета за электричество, злоумышленники используют для добычи криптовалюты вредоносное ПО, работающее на ресурсах других людей. Объединяя ресурсы нескольких зараженных устройств, киберпреступники могут создавать массивные сети для майнинга из сотен или даже тысяч устройств.

На майнинге криптовалюты преступники зарабатывают большие деньги. Согласно недавнему отраслевому отчету, 175 миллионов долларов в валюте Monero (5% от всего объема Monero в обращении) были добыты незаконно с использованием вредоносного ПО для криптомайнинга. Но, учитывая распространенность биткоинов и других криптовалют, общая сумма, вероятно, намного выше.

В отличие от явных атак программ-вымогателей, криптомайнинг трудно обнаружить. Хакеры маскируют вредоносное ПО для добычи криптовалюты под обычный сетевой трафик. В результате уровень заражения в 2018 году вырос более чем на 4000%, согласно данным McAfee, и многие компании могут быть заражены, даже не осознавая этого.

Решения Varonis не только помогли заказчику обнаружить угрозу, но также устранить это вредоносное ПО и защитить от будущих атак.

> “Мы понимали, что у нас есть проблема, но без Varonis мы бы так и не узнали, насколько она разрушительна.

Решение

ОПРЕДЕЛЕНИЕ МАСШТАБА ЗАРАЖЕНИЯ

Среди других решений безопасности заказчик выбрал Varonis по двум причинам:

1. Заказчик оценил Varonis на этапе пилотного проекта и понимал, насколько он эффективен при обнаружении и устранении потенциальных угроз.
2. Заказчик оценил открытый и честный подход команды Varonis как на этапе подготовки к сделке, так и после нее.

> “Многие поставщики решений просто хотели нам что-то продать. Они говорили «мы это видели много раз» или «мы можем решить эту проблему», не проводя дальнейших исследований. Но когда мы показали проблему команде Varonis, они сказали: «Мы такого раньше не видели».”

Чтобы выяснить, в чем заключалась угроза и как ее остановить, специалисты Varonis совместно с сотрудниками отдела безопасности заказчика исследовали масштабы заражения.

> “Команда Varonis не предлагала непродуманных решений: они выслушали, сделали заметки, подготовились и вернулись с обоснованными предложениями, которые помогли решить нашу проблему. Это был очень необычный подход.”

Анализ собранных образцов вредоносного ПО выявил его новый штамм, который исследовательская команда Varonis назвала «Норман». Он смог обойти **антивирусы, системы обнаружения сложных угроз на конечных точках (EDR) и межсетевые экраны**, эффективно избегая обнаружения в сети.

Другими словами, даже несмотря на то, что заказчик применял серьезные меры по защите, эта вредоносная программа смогла заразить почти все устройства до того, как была обнаружена.

ИСПОЛЬЗОВАНИЕ ПРОДУКТОВ VARONIS ДЛЯ УСТРАНЕНИЯ УГРОЗЫ

Три продукта Varonis помогли заказчику найти и исправить зараженное вредоносное ПО: DatAdvantage, DatAlert и Edge.

DatAdvantage представил клиенту подробную и наглядную информации о том, что происходит на его серверах и в облаке. Это позволило легко увидеть, когда и где происходят изменения и кто их вносит.

> “Каждая организация должна использовать DatAdvantage. Его панель мониторинга отображает информацию практически в реальном времени, а также аналитические данные, которых нам так не хватало. С помощью этого модуля мы можем отслеживать общие файловые ресурсы и службы каталогов, а также Office 365 и Azure.”

Используя DatAdvantage совместно с **DatAlert**, специалисты отдела безопасности смогли определить источники потенциальных угроз. Дополнительный контекст данных об этих угрозах позволил отделу безопасности понять проблему и предпринять быстрые действия.

> “Мы используем DatAlert ежедневно. Он предупреждает нас о подозрительной активности и позволяет найти источник проблемы — имя пользователя, компьютер или IP-адрес, которые с ней связаны. Это особенно важно, если злоумышленник использует разные географические координаты и прочие уловки.”

Кроме того, для обнаружения вредоносного ПО и борьбы с ним ценным оказался модуль **Edge**. Анализируя активность на устройствах периметра и активность доступа к данным, Edge смог обнаружить эту почти невидимую угрозу и предотвратить ее распространение.

> Что касается решений, Varonis Edge стал для нас самым ценным продуктом. Edge направляет нас к компьютерам с подозрительными DNS-запросами, сопоставляя их с конкретными пользователями и показывая нам адреса, которые нужно заблокировать.

> Команда Varonis не предлагала непродуманных решений: они выслушали, сделали заметки, подготовились и вернулись с обоснованными предложениями, которые помогли решить нашу проблему. Это был очень необычный подход.

Полученные результаты

ВЫЯВЛЕНО И УСТРАНЕНО ВРЕДОНОСНОЕ ПО

В течение нескольких месяцев в среде компании велась скрытная вредоносная деятельность. С помощью Varonis специалисты отдела безопасности смогли выявить эти действия, найти источник проблемы и удалить вредоносное ПО с каждого устройства.

> Varonis показал нам всю глубину проблемы и сыграл важную роль в ее устранении.

После устранения вредоносного ПО Varonis продолжает обеспечивать ежедневный мониторинг и защиту данных, обнаружение угроз и реагирование на них, а также соблюдение нормативных требований.

> Varonis позволяет легко найти информацию, которую обычно очень сложно найти. За считаные минуты мы можем точно узнать, кто получил доступ к общей папке, и принять меры в случае обнаружения подозрительной активности.

Заказчик оценил, что на панели мониторинга Varonis в режиме реального времени отражаются самые важные показатели, с помощью которых можно отслеживать потенциальные угрозы и уязвимости.

> Веб-интерфейс решения интуитивно понятен, а основные аспекты работы системы и создание отчетов можно подробно изучить в справке по продукту. Панель управления же позволяет быстро узнать, что происходит в вашей сети.

С тех пор компания попробовала в работе все продукты Varonis и охотно их рекомендует.

> Мы протестировали каждый продукт Varonis и, если бы у нас был неограниченный бюджет, мы бы внедрили весь стек решений.

“

Varonis показал нам всю глубину проблемы
и сыграл важную роль в ее устранении.

Не позволяйте вредоносному ПО преодолеть ваш периметр защиты

Защитите свою сеть
и ее периметр от угроз с Varonis.

ЗАПРОСИТЬ ДЕМОВЕРСИЮ